TRUCOS: HAZ COPIAS DE SEGURIDAD DE TUS CUENTAS GMAIL

Año XI 125
4,95€

@RROBA

LA REVISTA ESPAÑOLA MÁS VETERANA DE INTERNET Y SEGURIDAD INFORMÁTICA

8 414090 201599 00125

BORRADO SEGURO
Todos los métodos para que los datos desaparezcan para siempre

HACK WIFI
Seguimos instalando una red inalámbrica a medida

FANFILMS
El cine más sorprendente lo haces tú

JOHN THE RIPPER
Un clásico que sigue vigente

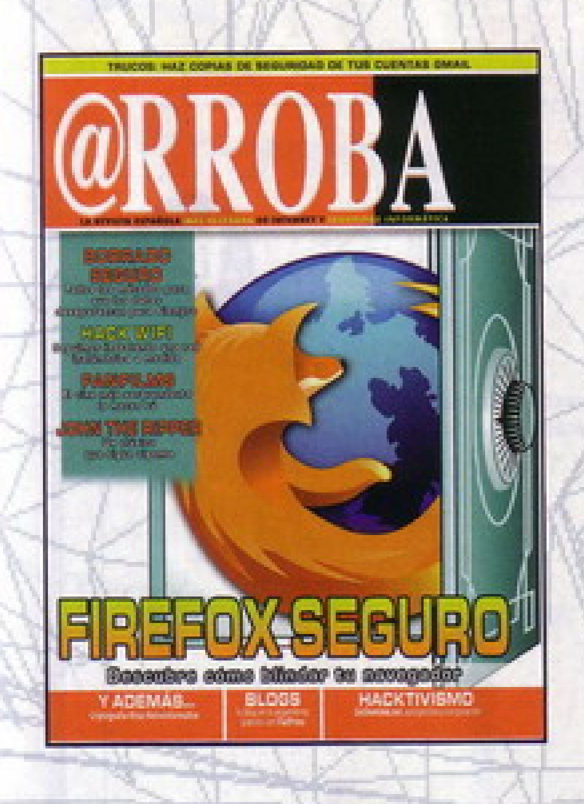


FIREFOX SEGURO
Descubre cómo blindar tu navegador

Y ADEMÁS...
Criptografía-Virus-Retroinformática

BLOGS
Tu blog en tu alojamiento gratuito con FlatPress

HACKTIVISMO
SinDominio.net, autogestión y cooperación



PRESIDENTE DEL CONSEJO EDITORIAL MARICRUZ MONTOYA LINARES/
COORDINADOR DE PRODUCCION FRANCISCO PEDREGAL BUENO/
DIRECTOR GABY LÓPEZ
REDACTORES ANDRÉS MÉNDEZ/ MANUEL BALERIOLA/ NICOLÁS VELÁSQUEZ/ SET/ SPARKRISP / MERCÈ MOLIST / PEDRO PERIS / NETTING / RAMIRO CANO / ENRIQUE ANDRADE
DISEÑO: DPTO. PROPIO
@LGARROBA DIRIGE:GABY LÓPEZ
COORDINACIÓN DEPARTAMENTO MAQUETACIÓN: GEMA BARBA
DPTO. DE SUSCRIPCIONES suscripciones@csr71.com

PUBLICIDAD: CENTRAL MEDIA YOUNG BARCELONA
AVDA. MERIDIANA 350, 5ºA - 08027 BARCELONA
TELF.: 93 274 47 39-FAX: 93 346 72 14

@RROBA
arroba@megamultimedia.com
arroba2@megamultimedia.com
Megamultimedia, S.L.
Paseo de Reding, 43, 1º
29016 Málaga
Teléfono: 952 36 31 43

DISTRIBUIDORA INTERNACIONAL
COEDIS

PRINTED IN SPAIN
II/MMVIII

ISSN-1138-1655
Dep. legal MA-1049-97 / nº125

ERAS TÚ MI ARTISTA PREFERIDO

Hay muchas cosas alarmantes y desquiciantes de todo el asunto que ha llevado a la aprobación del maldito canon. Una de ellas es la variedad de posturas de los artistas a la hora de justificar lo injustificable. Los hay que ponen cara de pena, como si nos quisieran hacer creer, por enésima vez, que el canon es una especie de cartilla de racionamiento que les permite tener su bollo del día, o que el canon es un derecho inalienable, sin el cual no podrán sacar el próximo disco u, horror, pagar la letra del piso. En el otro extremo, los desafiantes. No sabemos si son conscientes o no de que están repartiendo cera de forma indiscriminada entre sus propios seguidores, que han comprado sus discos e ido a sus conciertos. Quizá es que no les importa, y se lanzan a tumba abierta en un intento de reafirmarse a sí mismos. Pero el ridículo que están alcanzando empieza a ser reseñable. No es que estén mordiendo la mano que les da de comer, es que están haciendo que mucha más gente de la que se piensan les dé la espalda. Por último, los hay que justifican la existencia del canon, quizá sin tanta vehemencia ni queriendo inspirar pena, pero desafortunadamente sus argumentos siguen siendo erróneos, aunque se agradece que no los esgriman escupiendo a cámara. A todos les convendría ponerse en el lugar de sus seguidores, algo que ellos llevan pidiendo a los supuestos piratas, pero para llevarlos a su terreno y acorralarlos con soflamas incomprensibles. Incomprensibles porque está demostrado que hay formas de promover la cultura, y vivir de ello sin tener que cabrear a un buen porcentaje de su público potencial. La llamada era digital se concibe para abrir puertas, y hay quien se las está cerrando por puro miedo y pura codicia.

[SUMARIO número 125]



El Canon aprobado por el PSOE con el apoyo de IU incrementara en más de un 25% el coste de los productos y soportes electronicos

El Canon aprobado por el PSOE con el apoyo de IU incrementará en más de un 25% el coste de los productos y soportes electrónicos

- Los equipos electrónicos afectados por el nuevo Canon tendrán subidas de precio cercanas al 20% mientras que los soportes (CD, DVDs, Tarjetas) incrementarán su precio en más de un 40%

- Los partidos minoritarios CIU, ERC, PNV e IU dieron un giro radical en sus posiciones y acabaron imponer junto con el PSOE el canon digital. El Partido Popular se posiciona en contra del Canon Digital.

- El sistema propuesto ha sido cuestionado incluso por los que lo han aprobado que lo tachan de transitorio e imperfecto.

La plataforma todoscontraelcanon.es ha valorado positivamente la situación creada tras la aprobación del Canon digital en el último pleno de la legislatura gracias al cambio de postura de los partidos minoritarios que han cambiado el voto que habían emitido en el Senado tan solo hace unos días, como el principio del fin del canon digital, por los siguientes motivos:

En apenas tres días se han enviado 17.000 correos electrónicos los diputados y se han recogido más de 150.000 firmas en contra del canon digital, 50.000 de ellas el día en que se debatía su eliminación del congreso.

El debate sobre el canon digital ha tomado un enorme protagonismo, lo impopular de esta medida es evidente con un rechazo superior al 96% en todos los sondeos realizados y por tanto, no guarda relación lo votado en el Congreso de los diputados, que de forma inexplicada por inexplicable han dado la espalda a las demandas de la mayoría social.

Los partidos a favor del canon deberán explicar a sus electores, el motivo de apoyo de esta tasa arbitraria, indiscriminada e injusta.

Un denominador común denominador en todas las intervenciones, ha sido la necesidad de que la gestión de la recaudación de sociedades de gestión tenga mayor transparencia, incluso sea un organismo publico quien adquiera esas competencias.

Por otro lado, varias organizaciones tienen previsto oponerse a la implantación de este impuesto en el próximo Consejo de Consumidores y Usuarios, mientras que la plataforma Todos Contra el Canon seguirá movilizada. Tras conocerse el resultado en el Congreso, el universo de los blogs se convirtió en un hervidero. Las críticas de los internatuas han comenzado a dirigirse a los partidos que como el PSOE e IU han apoyado el canon, y no solo a la SGAE. Está por ver si el enfado se refleja el próximo 9 de marzo en las urnas.



Nuevas acciones de la plataforma todoscontraelcanon.es
La plataforma ha anunciado que se constituirá en Asociación con personalidad jurídica propia lo cual le permitirá desarrollar acciones legales con personalidad propia.

Acciones a tomar por la Plataforma.

Además de continuar con la recogida de firmas desde la plataforma, se han anunciado las siguientes iniciativas a desarrollar durante 2008:

Denunciar ante Defensa de la Competencia por la desproporción del canon en relación a los precios de los soportes y equipos, a partir de la puesta en marcha de la orden del Gobierno que supone en algunos casos un sobreprecio del 40% sobre el precio actual.

Denunciar la subvención cruzada de organismos públicos a entidades privadas derivadas del pago del canon por actividades desarrolladas por empresas y administraciones que nada tienen que ver con la copia privada tal y como recomienda la Comisión Europea.

Exigir a la inmediata retirada de los soportes originales con derechos de autor, que contengan protecciones anticopia que vayan grabados sobre soportes que hayan pagado un canon y que por tanto deben de poder ser copiados.

Exigir la puesta en marcha de un organismo público que se ocupe de la recaudación del Canon digital.

Exigir el desarrollo de los mecanismos reglamentarios que permitan desarrollar el apartado donde se dice literalmente "que si el perjuicio causado al titular de los derechos de autor es mínimo no podrá dar origen a una obligación de pago".

Un impuesto injusto y poco democrático
"En el modelo propuesto los ciudadanos vamos a pagar por nuestras fotografías, por hablar por teléfono o por escribir nuestros correos, las administraciones públicas van a subvencionar directamente la actividad de entidades privadas como son las entidades de gestión en razón de una copia privada que no hacen, algo que atenta contra todos los principios democráticos" afirman los miembros de la todoscontraelcanon.es

Por otro lado se proponen importes fijos sobre los productos y soportes algo tremendamente peligroso ya que esto, tal y como ha sucedido en CDs y DVDs, ha obligado al cierre de todas las empresas que fabricaban estos productos e incentivado el mercado negro de dichos productos. Esta norma, hoy publicada, significa que dentro de unos años productos como los MP3, las tarjetas de memoria o los móviles se compraran en el mercado negro por el sobre coste del canon.

Existe una solución
La solución al Canon, propuesta por la plataforma todoscontraelcanon, es que este se cobre directamente sobre la obra que lo genera y no en los equipos y soportes dónde se reproduce. "Esta solución es justa y sencilla ya que cada cual cobra por su trabajo y lo carga en sus productos y no en los de terceras partes, esperamos que este Jueves los diputados y los partidos políticos apliquen el sentido común y no se dejen llevar por la presión de los intermediarios que son los que realmente se benefician de un canon indiscriminado."



Hack wifi

(Parte XXI)

Diseño e Instalación de una red inalámbrica a medida II

Seguimos donde lo dejamos el mes anterior, donde os recuerdo que hicimos un pequeño descanso para acercarnos al diseño e instalación de un red inalámbrica a medida. En el artículo pasado, por falta de espacio, no pudimos finalizar la explicación y tuvimos que posponerlo para este número. En este capítulo de Hack Wi-Fi finalizaremos con la explicación, tocaremos temas muy importantes a lo que se refiere a redes locales y os presentaré una nueva herramienta muy interesante a la hora de hablar de auditoria inalámbrica.



Metidos de lleno en el 2008. Si, lo sé. Ya estamos en Febrero. Lo que ocurre es que yo me atraso a los acontecimientos, recordar que desarrollo los artículos un mes antes de ser publicados. Por lo tanto, siempre se me pasan algunas cosas... Este artículo que hoy tienes en tus manos lo he escrito a mediados de Diciembre. Ya te das cuenta del motivo ¿verdad?. Pues nada, que no quería yo terminar el año sin dar la bienvenida al 2008 a mis lectores y deciros: "Feliz Navidad".

También me gustaría daros las gracias a todos aquellos lectores que seguís de cerca todos mis artículos, que me constan que no sois pocos. Con este mes, cumplo ya 3 añazos trabajando para la revista @rroba. Ha sido todo un placer trabajar con esta editorial todo este tiempo... y el que nos queda todavía d:b.

Antes de empezar con el artículo me gustaría enviarle un saludo y un fuerte abrazo al que fue durante un buen período de tiempo el director de la revista @rroba. Un saludo Carlos Verdier, ha sido todo un placer trabajar contigo durante estos dos últimos años.

Venga, sin más preámbulos entramos en materia:

Como os decía en la introducción del artículo este mes, vamos a finalizar con las explicaciones que comenzamos el mes anterior, también os presentaré una nueva herramienta la mar de interesante a la hora de hablar de auditorias inalámbricas. ¿Qué tal si empezamos por aquí?

Live CD Black | Track BETA 3

Black | Track BETA 3 es un Live-CD desarrollada para la auditoria de seguridad informática.

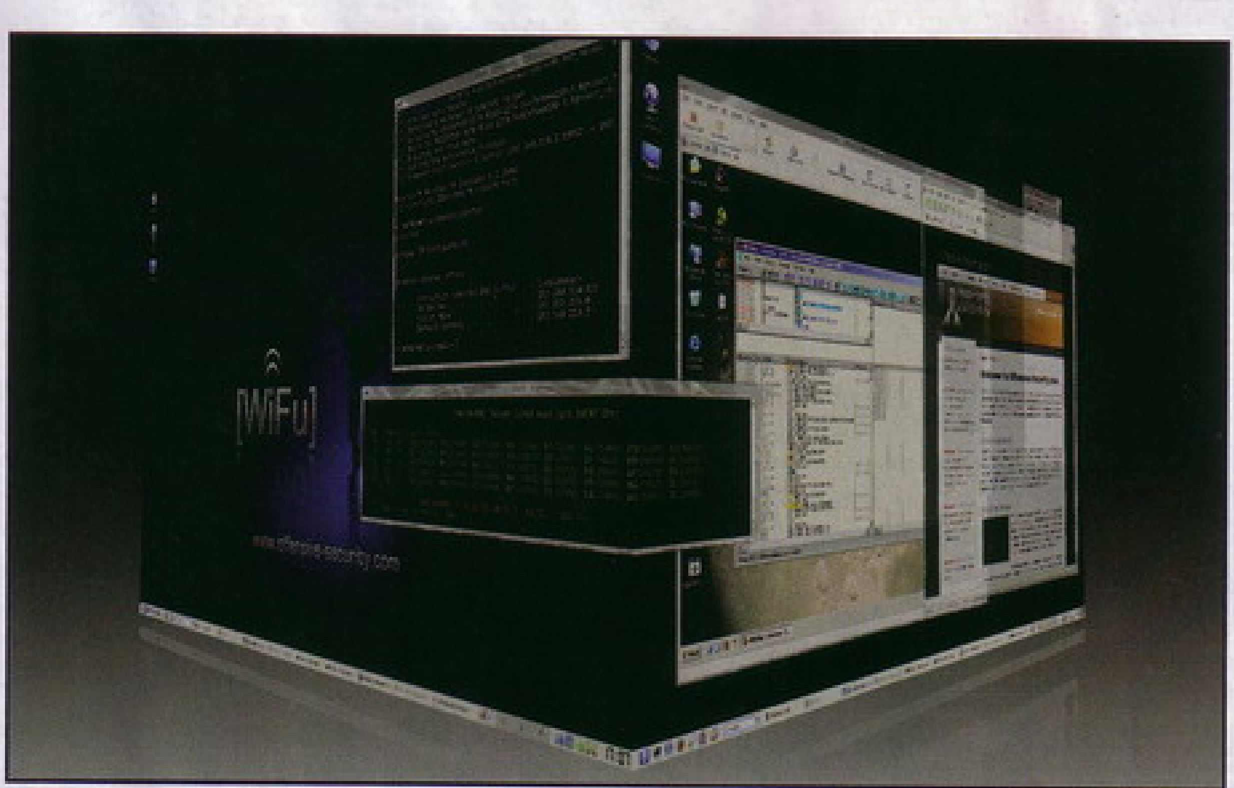
Esta versión fue liberada a mitades de Diciembre del 2007. Dispone en su interior de más de 300 herramientas dedicadas a la seguridad informática. Entre ellas encontramos muchísimo material para la auditoria inalámbrica o para el Hacking Wireless.

Podéis comprobar por vosotros mismos todas las herramientas disponibles en este Live-CD en la siguiente dirección: http://backtrack.offensive-security.com/index.php?title=Tools

Esta nueva versión dispone de muchas mejoras y muchas novedades interesantes:

- Utilización del Kernel 2.6.15.5. Que supone un mejor soporte para procesadores Core Duo.

- Un aumento considerable para la compatibilidad de tarjetas inalámbricas. Pode-









mos comprobar en la siguiente URL todas aquellas tarjetas inalámbricas soportadas: http://backtrack.offensive-security.com/index.php/HCL:Wireless . Que como comprobaréis no son pocas.
- Soporte para booteo PXE en red para el modo CLUSTER. Por cierto, interesante opción.
- Suite de Metasploit Framework actualizada.
- Cracking simultaneo de máquinas en modo Cluster con John The Ripper
- Drivers Nvidia agregados.
- Save2CD. Que esta vez funciona perfectamente.

Entre otras muchas y muchas cosas más.

Este Live-CD está liberado en dos posibles opciones:

- Por un lado: Un Live-CD en formato ISO de 700 MegaBytes. Que podéis y debeis descargaros desde aquí: ftp://bt3.aircrack-ng.org/bt3b141207.iso

- Y por otro: Para dispositivos USB, mucho más completa que la imagen anterior. De unos 946 MegaBytes. Que podéis descargaros desde aquí: ftp://bt3.aircrack-ng.org/bt3b141207.rar

Lástima que no disponga todavía de una unidad USB portable de 1 o 2 Gigabytes :b

Por lo que he escuchado "por ahí" los autores prometen que pronto publicarán una presentación de 1 GigaByte en formato DVD, y que no esperan que haya fallos en ella...

Si. Como todo en esta vida, nada es perfecto. Aquí os dejo para los interesados los bugs que tiene el Live-CD: http://wiki.remote-exploit.org/index.php/Bugs

Si quereis más información al respecto, disponéis de un wiki oficial: http://wiki.remote-exploit.org/index.php/Bugs

Para los que os gusten el cine en casa os dejo un video de Live-CD Black | Track en plena accción: http://www.ethicalhacker.net/content/view/167/1/

La página oficial del proyecto: http://www.remote-exploit.org/backtrack.html

Venga... decirme que no es para chuparse los dedos : b

Supongo que a estas alturas ya estará disponible un proyecto que estamos desarrollado en: http://www.wadalbertia.org. Un proyecto muy interesante, portable, potente y eficaz. En otro artículo estoy seguro de que os hablaré de el. Si no podéis esperar visitar mi blog: http://blog.netting.es el foro http://foro.netting.es o la comunidad de Wadalbertia http://www.wadalbertia.og seguro que allí encontraréis información muy interesante acerca del proyecto. ¡¡ Estar atentos !!

Pasemos ahora con la parte que nos quedaba por explicar del diseño e instalación de una red inalámbrica a medida.

RECORDAR QUE SI EL AP B ESTÁ TRABAJANDO COMO CLIENTE DEL AP A, NO PODREMOS CONECTARNOS AL AP B MEDIANTE UNA CONEXIÓN INALÁMBRICA

Parte 2 - WLAN a MEDIDA

Recordemos cuales eran los objetivos que perseguimos. Seguro que estamos un poco perdidos.

El objetivo era, desarrollar una determinada instalación inalámbrica y cableada para unir dos redes locales diferentes por tecnología Wi-Fi.

Lo que me proponían es lo siguiente:

En este AULA tenemos una conexión a Internet de 6 megas... El aula está compuesta de unos doce ordenadores de sobremesa y de unos cuatro o cinco portátiles. Conectados entre si por un Switch y un AP (Punto de Acceso). Los ordenadores de sobremesa se conectan a través del Switch y los portátiles a través del AP.

Queremos conectar este AULA con una segunda AULA continua a esta. Esta segunda AULA, a partir de ahora AULA B, dispone de una red local mayor, con más máquinas y dispositivos que la interconectan. Aunque más adelante nos centraremos en su arquitectura física, su composición y como está configurada, haremos una pequeña descripción de cómo está organizada el AULA B.

El AULA B dispone de unos veinticinco ordenadores de sobremesa con distintos sistemas operativos instalados (Windows 2000 Profesional, Windows 2000 Server, Windows 2003 Server e incluso varias distribuciones de GNU/LiNUX, Ubuntu). La red está compuesta de unos cinco Switchs, un AP y dos Routers neutros, dos Linksys WRT54G v.5 con el software por defecto.

Lo que se me proponía era unir las dos redes locales. Que el AULA B pudiese conectarse con el AULA A y salir a Internet a través de esta.

Las condiciones eran las siguientes:

- Deben de ser dos subredes diferentes.
- Deben de utilizar diferentes direcciones IP para cada subred. Principalmente para que no haya problemas de solapamiento de direcciones IP entre las clases.
- Cada subred debe de ser independiente de la otra, exceptuando la salida a Internet, que debe de ser compartida.
- La instalación del primer AULA no debe de modificarse, exceptuando la configuración del AP.
- La conexión entre las dos AULAS debe de ser por tecnología Wireless.
- Aplicar la máxima seguridad posible.
- La conexión Wireless debe de ser entre dos APs de la misma marca. Simplemente, para adaptarse a el equipamiento del AULA. Estos APs son Robotics.
- La asignación de direcciones IP, Máscara de subred, puerta de enlace, Servidores DNS (principal y secundario) debe de ser manual, no a través de un servidor DHCP. Básicamente para administrar los alumnos sus conexiones de red.
- En el AULA B no tendrá una conexión Wireless.
- El AULA A tendrá conexión Wireless.

En el artículo del mes anterior explicamos todo lo necesario para conectar dos puntos de acceso. Que si uno trabaja en modo infraestructura, que si el otro trabaja en modo cliente., etc, etc.

Al final del artículo habíamos conseguido conectar el AP del AULA B con el AP del AULA A. Y por extensión, conectando un PC por cable al AP del AULA B tener acceso a cualquier máquina del AULA A, así como salida a INTERNET.

MUSICA ORIGINAL

CONVIERTE TU MOVILE EN UN MP3 PORTATIL

sms envía **MUSICA19** (espacio) **código** de cancion **al 7494**

EJEMPLO: para descargarte LA SINTONIA de los SIMPSONS tienes que enviar MUSICA19 26189 al 7494

Rechaza imitaciones

7310	HIMNO REAL MADRID HALA MADRID!	Himno
3679	EL PADRINO	Nino Bravo
3680	EYE OF THE TIGER (BSO ROCKY III)	BSO Rocky III (Survivor)
1486	ME MUERO	La Quinta Estación
30614	Y AHORA VOY A SALIR (RANXEIRA)	Mago de Oz
0358	ATREVETE-TE	Calle 13
31419	WHEN I´M GONE	Simple plan
26122	ACABO DE LLEGAR	Fito y Fitipaldis
6701	HIGHWAY TO HELL	ACDC
27415	1973	James Blunt
28507	BEAUTIFUL GIRLS	Sean Kingston
6664	REGRESA A MI	Il Divo
3677	BSO GLADIATOR	Hans Zimmer
17452	ADOLESCENTES	Kiko y Shara
31149	THE WAY I ARE	Timbaland
7186	BSO LA PANTERA ROSA	Henry Mancini
13552	QUE HICISTE	Jennifer López
13588	QUIEREME	Andy y Lucas
9908	COMO EN UN MAR ETERNO	Hanna
25394	COMO LA VIDA (VUELTA CICLISTA 07)	Hanna
13884	MICROMANIA	Tata Golosa
1593	TU RECUERDO	Ricky Martin con Chambao
3694	EVERY BREATH YOU TAKE	The Police
65453	NO ONE	Alicia Keys
13068	SALIO EL SOL	Don Omar
4887	BSO FRAGGLE ROCK	
13567	HOW TO SAVE A LIFE (BSO ANATOMIA DE GREY)	The Fray
13763	PEGATE	Ricky Martin
14244	ALL GOOD THINGS	Nelly Furtado
1488	SUEÑOS ROTOS	La Quinta Estación
2340	MAIN TITLE (BSO EL ULTIMO MOHICANO)	Jones y Edelman
17591	SER O PARECER	RBD Rebelde
29960	AGUITA DE ABRIL	María
7548	SWEET CHILD OF MINE	Guns N Roses
29759	HASTA LLEGAR A ENLOQUECER	Diego Martín
27692	APROXIMACIÓN	Pereza
13073	GRACE KELLY	Mika
9481	POR LA BOCA VIVE EL PEZ	Fito y Fitipaldis
31288	NO VOY A CAMBIAR	Malú
2766	AROUND THE WORLD	Daft punk
31337	LA CIUDAD DE LOS ÁRBOLES	Mago de Oz
8997	LABIOS COMPARTIDOS	Maná
9100	PULP FICTION	BSO Pulp Fiction
17743	BLEED IT OUT	Linkin Park
29735	POR TI DARIA	Hanna
31234	INALCANZABLE	RBD Rebelde
14609	PARA TODA LA VIDA	El Sueño de Morfeo
0917	SMACK THAT	Akon feat Eminem
2343	BSO GREASE	John Travolta y Olivia Newton John
3885	YOU'RE BEAUTIFUL	James Blunt
14358	MORENAMIA (DUETO 2007)	Miguel Bosé y Julieta Venegas
31218	CAL Y ARENA	Merche
3681	UNCHAINED MELODY (BSO GHOST)	The righteous brothers
28757	LA DOLCE VITA	Soraya
4901	BSO PRETTY WOMAN	Roy Orbison
25581	MY OWN WAY	Banghra
5725	ENTRE DOS TIERRAS	Heroes del Silencio
9030	NI UNA SOLA PALABRA	Paulina Rubio
13235	VUELVETE A LA LUNA	Shaila Dúrcal
26189	BSO LOS SIMPSONS	BSO Los Simpsons

Harry Potter y la Orden del Fénix

POLIFONICOS



ÚSALOS COMO TONOS DE LLAMADA PARA TUS AMIGOS

sms envía **TONOS4** (espacio) **código** polifonico **al 7494**

EJEMPLO: para descargarte "BSO DEL ZORRO" tienes que enviar TONOS4 92061 al 7494

bájate todos los éxitos ¡¡¡para tu móvil!!!

92747	Young folks
82172	Barcelona
83188	Real Madrid
89029	Himno España
89601	Himno O. Del Cent.Del Sevilla F.C.
84207	El Padrino
84724	BSO El bueno, el feo y el malo
92272	Umbrella
92463	África
85220	Himno de la legión
80082	BSO La pantera Rosa
85529	BSO El ultimo mohicano
92665	Me enamora
84094	Himno de riego
83227	Salve Rociera
85606	Vals de Amelie
84446	Cara al sol
84067	Tubular bells (BSO el exorcista)
84490	Asturias patria querida
84202	Telefono antiguo
92991	Gimme More
84759	Gladiator
92061	Amor gitano (BSO El Zorro)
82984	Paquito El Chocolatero
80108	Sintónia Benny Hill
80039	Eye of the tiger (BSO Rocky III)
83808	Himno de España
84560	Sintonia Curro Jimenez
85607	Sintonia El pajaro loco
84940	Sintonia cabecera Sexo en NY
80017	BSO Mision imposible
83883	Sintonia cabecera Fraggle Rock
84064	Darth Vader Marcha imperial
84966	24 - Serie TV
85333	You´ll never walk alone
84855	Amunt Valencia
84494	La internacional
89849	Para que tu no llores
90283	Como en un mar eterno
82124	Atletico De Madrid
82123	Athletic De Bilbao
84436	Centenario Real Madrid
83648	Sintonia La familia Monster
91237	Me muero
92898	No Estamos Solos (Non Siamo Soli)
83737	Dragon Ball Z
84692	Sintonía cabecera Rasca y pica
82873	Muñeira De Chantada
83326	Soy Minero
83901	Zorba el griego
84440	El señor de los anillos
80096	BSO Pulp Fiction

ATENCIÓN AL CLIENTE 902 01 30 16 (10 - 19 horas)



JUEGOS

Descárgatelos al móvil y juega donde y cuando quieras

sms envía **JUEGOS30** (espacio) **código** juego **al 7494**

EJEMPLO: para descargarte "BISBAL FAN FACTOR" tienes que enviar JUEGOS30 3094 al 7494

convierte tu móvil en una consola de juegos



código 3118

MOBILE BODY TRAINER entrenador personal físico

código 3098



código 3091

ZUMA

código 2034

Prepárate para una acción desbordante en tu móvil con este popular y adictivo juego de bolas. Controla la rana ídolo de piedra del antiguo Zuma en este emocionante juego de puzzle.¡No dejes que alcancen la calavera dorada o el juego se habrá terminado! De cualquier forma ya verás que no es fácil vencer en este simple, pero altamente adictivo juego para tu móvil.



código 1836

MIAMI NIGHTS

código 3035

DOGZ

código 3089



código 3025

¡Entrena tu mente y conviértete en el más listo de tus amigos!

BRAIN CHALLENGE

código 2616



código 3107

código 1435

TOP JUEGOS

3110	SONIA MONROY SEXY BLOCKS
5577	VIRTUA TENNIS MOBILE
3112	DESAFÍA AL INGLES
3120	REAL FOOTBALL 2008
3024	DESEOS OCULTOS
3113	MOVILMESSENGER
3093	MOBI LOVER
9585	SEXY VEGAS ANASTASIA MAYO
1051	BUBBLE BASH
1836	50 X 15
1435	REAL FOOTBALL 2007
1181	CONECTA 4
3109	SPYRO LA LEYENDA

PIN UPS DE FANTASIA

envía **FONDO39+** (espacio) **código** de la imagen **al 7808**





SONIBROMAS

sms envía **POLITONO83** (espacio) **código** polifonico **al 7808**

ÚSALOS COMO **TONOS** DE LLAMADA PARA TUS AMIGOS

31551	¿y tu porque no te callas?
30687	Himno Barsa
30762	Himno del Valencia
78849	Barça - Forza Barça
78862	Sevilla - Hasta la muerte
27457	Padre nuestro pijo
79089	Rianxeira
79098	Athletic, Athletic, Athletic!
78855	R. Madrid - Ya estamos todos aquí
78868	R.Madrid - Coge el móvil
77395	Mensaje del caudillo
77762	Como el luisma no se entera
8026	Toros Toque de corneta
78860	Betis - Sentimiento verdiblanco
79078	Racing, Racing, Racing!
78703	El Rey
79087	Alé Deportivo alé!
79094	Atleti, Atleti, Atletico de Madrid
79070	Alé Zaragoza alé

XMESSENGER

ahora para móviles

TUS CONTACTOS SIEMPRE CONTIGO



sms envía **MSX46** (espacio) **2269** al **7494**

MESSENGER EN TU MÓVIL



TEMAS

TEMA = FONDO + ICONOS

¡llénalo de coches tuneados!

Tuning World código 1582

sms envía **MENU26** (espacio) **código** del tema **al 7494**



Fantasmas código 0165



Culturistas código 13789



Recordar que si el AP B está trabajando como cliente del AP A, no podremos conectarnos al AP B mediante una conexión inalámbrica. Las interfaces inalámbricas están ocupadas, están conectadas con el AP B.

Aunque esto no es del todo cierto... Existe la posibilidad de indicar que interfaz (antena) trabaje como cliente y cual como infraestructura... Pero bueno, eso es otro tema que ya tocaremos en otro capítulo de Hack Wi-Fi.

El AP A seguirá estando disponible para todos los hosts que quieran conectarse a el mediante una conexión Wi-Fi. Recordar que este si que está trabajando en modo infraestructura.

Bien. Ahora tenemos que conectar el AP B con la red local cableada del AULA B.

Para ello he utilizado un Router Neutro Wi-Fi... Ya os imagináis que modelo he utilizado... ¿verdad?. Pues si. Un Linksys WRT54GL.

Este Router nos da un mar de posibilidad, ya no os digo si tiene instalado en su interior un sistema operativo GNU/LiNUX... Entonces haremos virguerías y cochinadas ;b

Pasemos a explicar cómo está físicamente conectada y orientada esta conexión.

LA ARQUITECTURA FÍSICA ES TREMENDAMENTE SENCILLA. TAN SOLO DEBEMOS DE CONECTAR MEDIANTE UN CABLE UTP 5 CONSTITUIDO POR DOS RJ45

Arquitectura física AP B – Router Linksys

La arquitectura física es tremendamente sencilla. Tan solo debemos de conectar mediante un cable UTP 5 constituido por dos RJ45, un extremo a la única boca del AP B y el otro extremo del cable a la boca INTERNET del Router Linksys (En la imagen ya os indico de qué boca se trata).

El AP B debe de estar lo más cerca posible del AP A. Mayormente para disponer de una mejor cobertura y evitar interferencias y solapamientos, que puede existir de todas formas. Creo que es bastante lógico, pero lo índico de igual forma, tenéis que evitar acercar los Puntos de Acceso a estanterías metálicas o cajas metálicas. De lo contrario, perderemos la mayoría de la señal y, en circunstancias totalmente desfavorables, perder totalmente la señal.

La distancia mayor que puede existir entre el AP B y el Router Linksys es de unos 100 metros de cable de red. Exceptuando, de si contamos con un dispositivo entre el AP B y el Router Linksys, por ejemplo un HUB, que extienda la señal. De este modo la distancia máxima de cable de red será de unos 200 metros.

Si. Se que a muchos puede pareceros una barbaridad y de poca utilidad utilizar una cable tan largo... pero a mi ya se me están ocurriendo algunas cosas, digamos interesantes, que podrían requerir un cable de red de estas dimensiones...

Y ahora la pregunta del millón... ¿Por qué un Router Neutro Wi-Fi? ¿Por qué un Linksys?

Empecemos por la primera pregunta, que ya fue contestada más arriba. Me gusta esta marca. Es un Router buenísimo que nos facilita muchísimo las cosas y por que podemos realizar con él casi cualquier cosa.

Necesitamos un Router, un enrutador, para poder enlazar las distintas redes LAN (AULA A – AULA B). Recordar que las dos redes utilizan diferentes direcciones IP y necesitamos "algo" que pueda comunicar/unir esas dos redes locales "diferentes" y encaminar enrutar conexiones, pues bien, eso es un Router... Espero que lo más puristas acepten esta simple definición... Lo importante es que lo entendamos todos ;)

Utilizamos un Router neutro porque al disponer de la boca INTERNET nos facilita muchísimo las cosas.

¿Wi-Fi? Pues para dar servicio inalámbrico (o no), eso ya es cosa del administrador de la red, pero la posibilidad está ahí.

Pasemos ahora a configurar la red local del AULA B para que pueda conectarse y salir a Internet desde el AULA A.

Configuración del Router Linksys

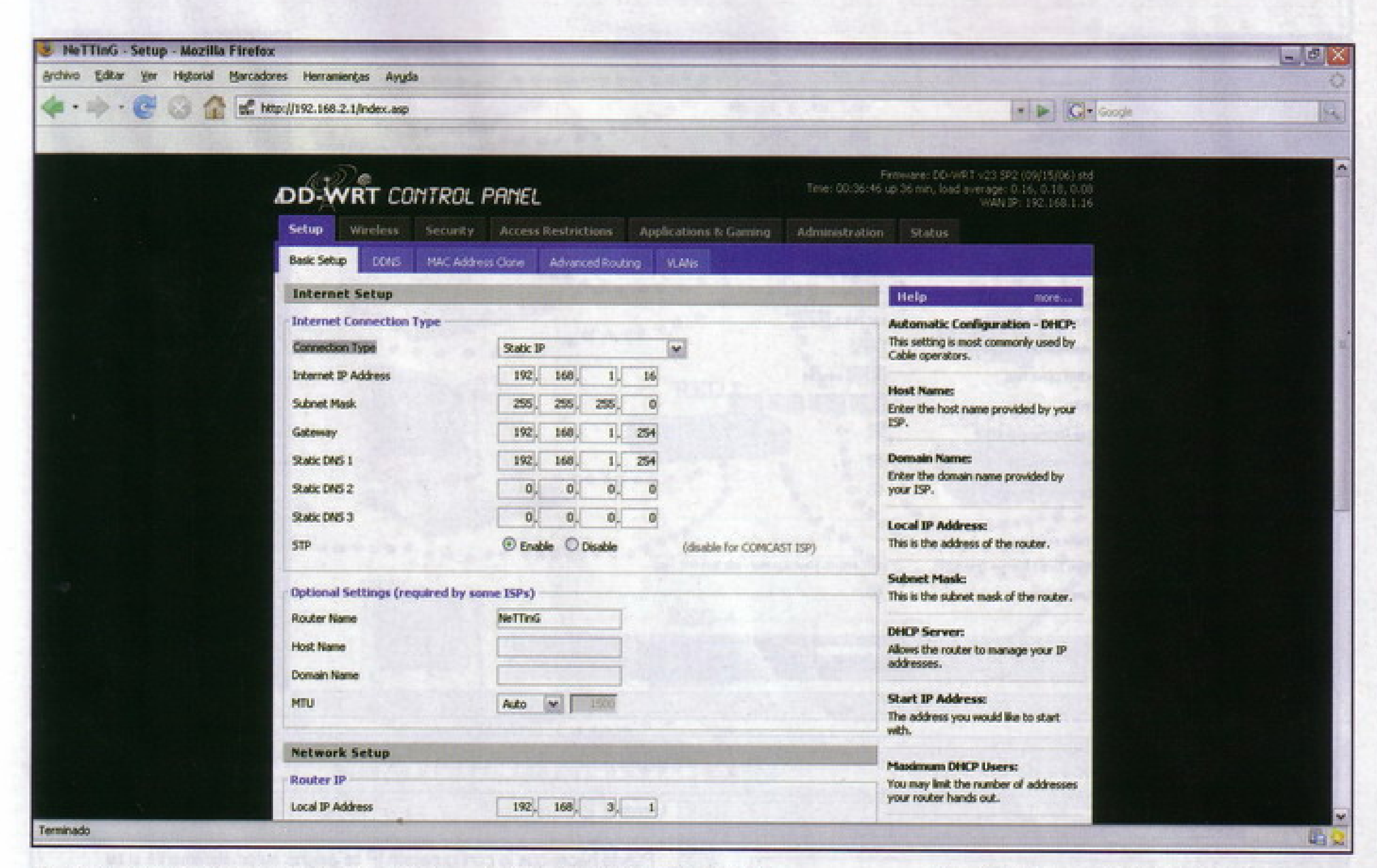
Vamos a configurar el Router Linksys mediante cable. Aunque bien podría configurarse mediante Wi-Fi.

Conectamos el cable UTP 5 con los conectores RJ45 a la boca de la tarjeta de red y el otro RJ45 a una de las bocas del Router Linksys.

Accedemos al Router mediante nuestro explorardor favorito:

http://192.168.1.1

Y es aquí donde podéis encontraros con varios problemas... Cada cual pue-



de tener configurado su Router "a su manera". Con una dirección IP diferente a la predeterminada (192.168.1.1). Con el Servidor DHCP deshabilitado. Con el Servidor DHCP habilitado. El Router trabajando en algún otro modo que no sea infraestructura... En fin, que hay para todos.

Si os acordáis de la configuración existen perfecto... Y si no, pues a tirar del botón "RESET" que acompaña a nuestro querido Router Linksys.

Una vez intentemos conectarnos con el Router nos pedirá que nos autentiquemos:

Usuario: root
Password: admin.

Esta es la configuración por defecto de la versión firmware: DD-WRT v23 SP2 (09/15/06) std (estándar).

Una vez dentro del aparato nos vamos a la pestaña: "Basic Setup" y pasamos a configurar cada opción:

Connection Type: Static IP.

Internet IP Address: 192.168.1.16

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.254

Static DNS: 192.168.1.254

LO QUE HEMOS CONFIGURADO ES EL ROUTER LINKSYS PARA QUE PERTENEZCA A LA RED LOCAL DEL AULA A. DE ESTA RED VENDRÁ LA CONEXIÓN A INTERNET

Esto que acabamos de configurar (Internet Setup), es la configuración de Internet. Aunque para este caso lo que hemos configurado es el Router Linksys para que pertenezca a la red local del AULA A. De esta red vendrá la conexión a Internet, de ahí que conectásemos la conexión recogida por el AP Robotics mediante Wi-Fi a la boca de Internet del Linksys.

Ahora nos queda configurar la parte Network Setup, que es la configuración de red local.

Router IP

Local IP Address: 192.168.3.254

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.254

Local DNS: 192.168.1.254

En el area Network Address Server Settings (DHCP):

DHCP Server: Disabled

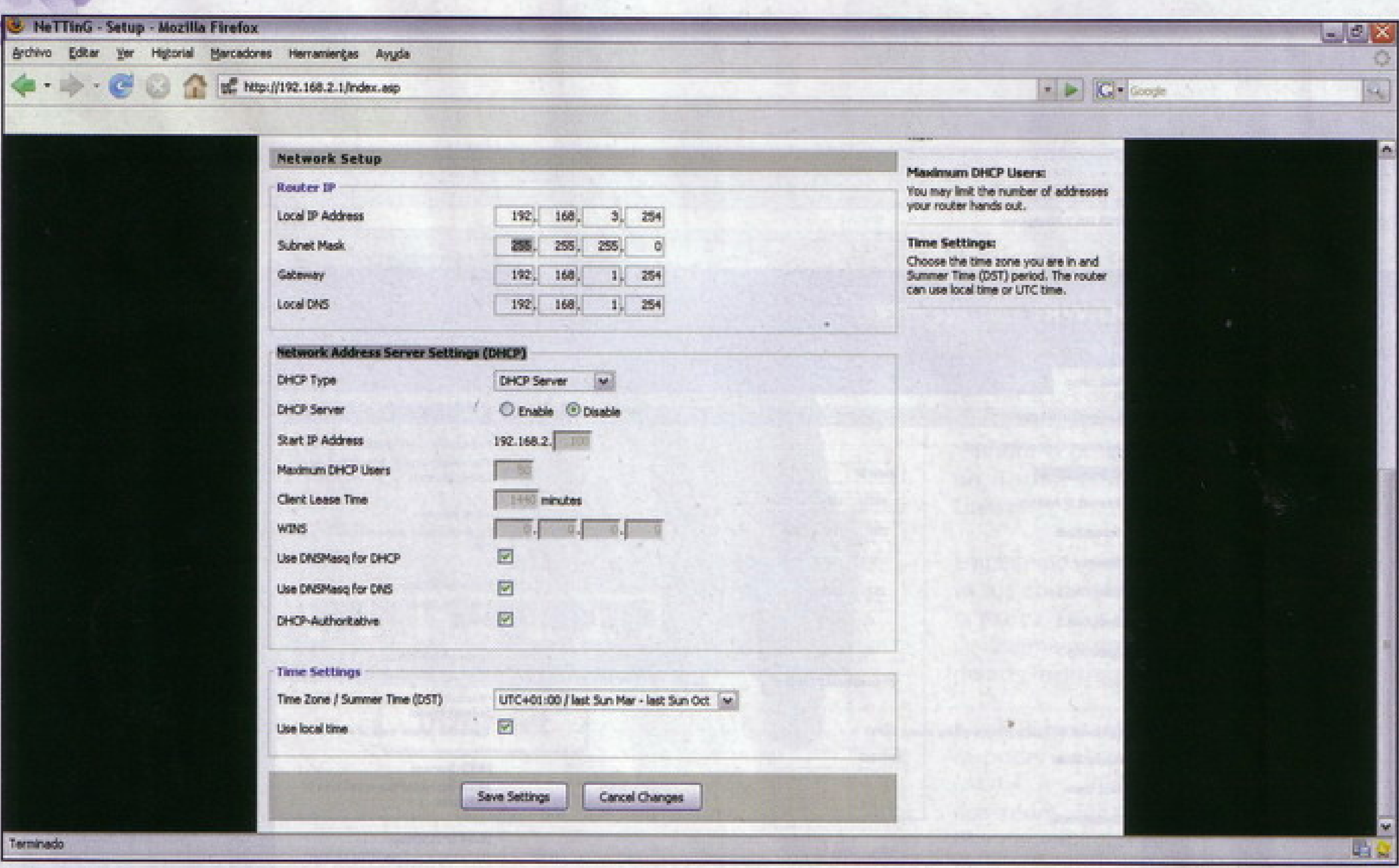
Como observaréis he utilizado la dirección IP: 192.168.X.254 para referirme a todos los Routers que componen la red.

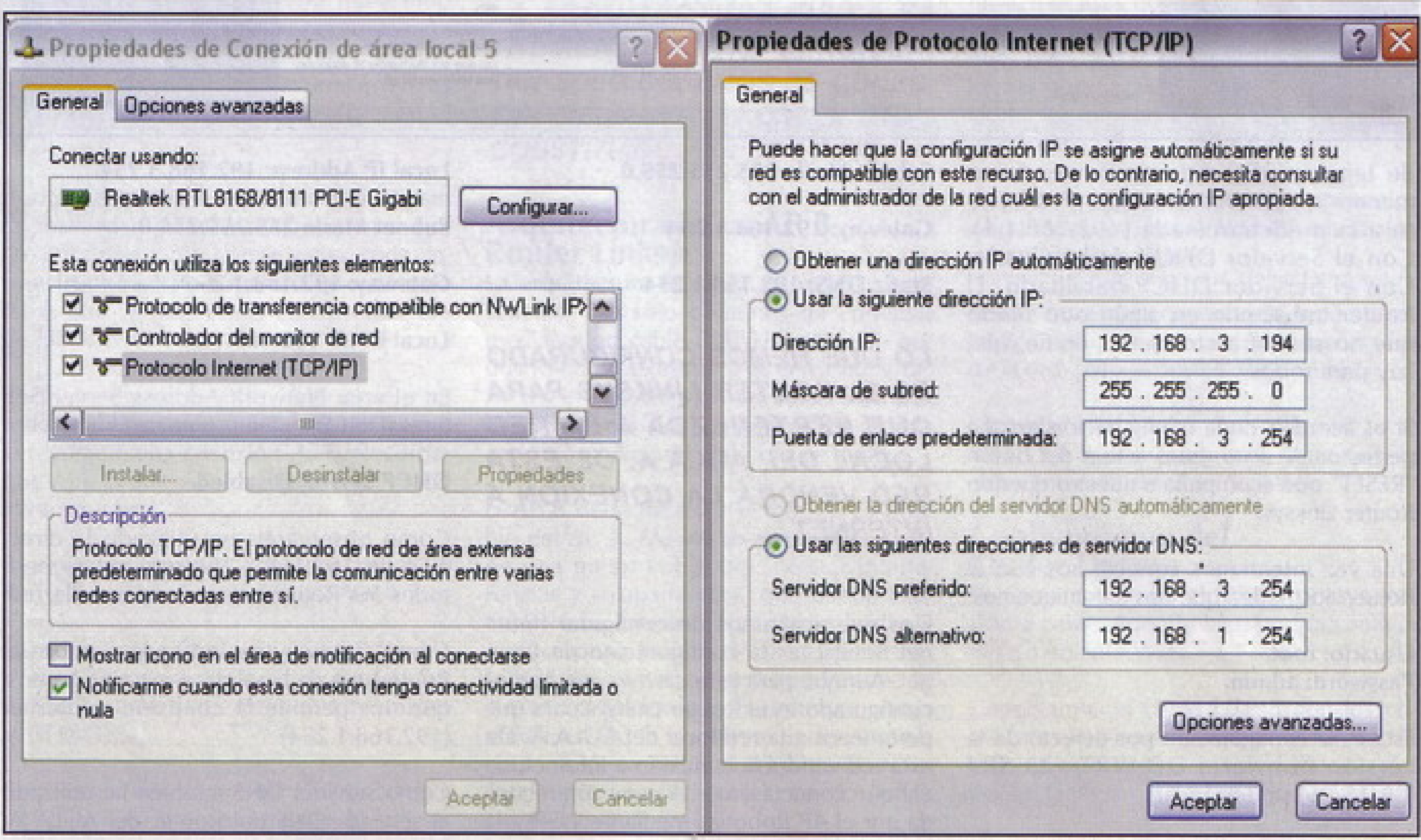
Como Gateway he indicado siempre el Router que da la salida al exterior, vamos, que nos permite la conexión a Internet (192.168.1.254).

Como servidor DNS también he utilizado el servidor DNS del Router del AULA A. De esta manera este será quien resuelva las peticiones DNS.

Y poco más hay que comentar...

Si ahora conectamos el Switch principal a una de las bocas RJ45 del Router Linksys





y configuramos cada PC de la red con la nueva configuración de red. Todos los dispositivos de la red del AULA B podrán salir a Internet:

Para que un PC del AULA B pueda salir a Internet o conectarse con un PC del AULA A debe de estar conectado con el Router Linksys, ya sea directamente o bien a través de otros dispositivos como HUBs y Switchs, que estén conectados con el Router Linksys.

Y tener la siguiente configuración de red:

Inicio - Panel de control - Conexiones de red

En la conexión de red, botón derecho, pro-



Arquitectura física - AULA B

PARA QUE UN PC DEL AULA B PUEDA SALIR A INTERNET O CONECTARSE CON UN PC DEL AULA A DEBE DE ESTAR CONECTADO CON EL ROUTER LINKSYS, YA SEA DIRECTAMENTE O BIEN A TRAVÉS DE OTROS DISPOSITIVOS

piedades. Protocolo TCP/IP, propiedades: Usar siguiente dirección IP:

Dirección IP: 192.168.3.X

Máscara de subred: 255.255.255.0

Puerta de enlace predeterminada: 192.168.3.254

Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido: 192.168.3.254

Servidor DNS alternativo: 192.168.1.254

Fijaros que la puerta de enlace predeterminada del AULA B es el Router Linksys, pues este es el enrutador que conecta las dos redes locales.

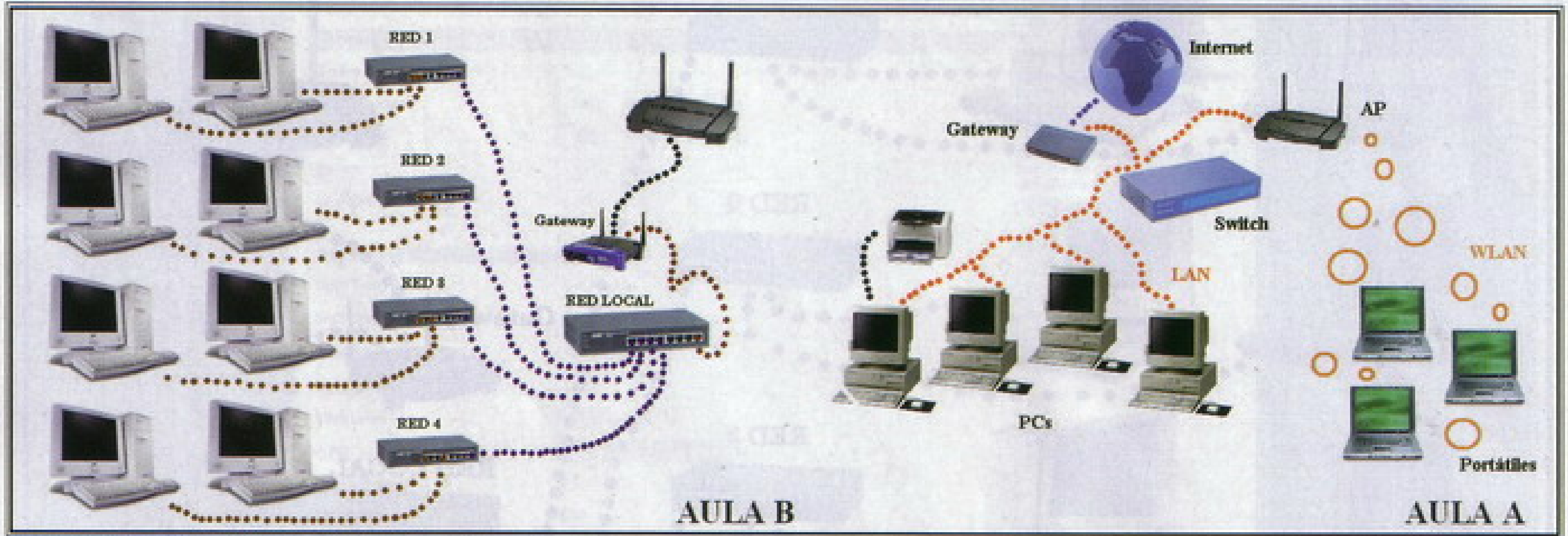
El servidor DNS es igual que sea la primera dirección IP que la segunda, todas las peticiones DNS las resolverá el Router del AULA A.

El AULA B quedaría de la siguiente forma (Imagen AULA B):

La red completa unida por los dos APs queda de la siguiente forma:

Por último nos quedaría instalar un cortafuegos en el Router Linksys, o bien en todos los PCs de la red con una directiva de seguridad determinada.

Lo más seguro, cómodo y recomendable es utilizar unas directivas de seguridad en el Router Linksys que permitan las conexiones del AULA B



Arquitectura física - AULA



hacia el Router (192.168.1.254) del AULA A. Y que denegarán las conexiones del AULA B hacia cualquier otro dispositivo del AULA A. De igual manera que denegase TODAS las conexiones del AULA A hacia el AULA B exceptuando las conexiones del Router del AULA A.

Si utilizásemos un cortafuegos por cada PC de la red local tendríamos que utilizar la siguiente directiva de seguridad:

AULA A:

Restringir todas las conexiones procedentes del AULA B al AULA A. Permitir todas las conexiones del AULA A.

AULA B:

Restringir todas las conexiones procedentes del AULA A al AULA B, exceptuando las conexiones del Router del AULA A. Permitir todas las conexiones del AULA A.

Esta política de seguridad se utilizaría en cada cortafuegos de cada PC que compone la red.

Conclusiones

Con este artículo terminamos con la parte de Instalación de una red inalámbrica a medida. Espero que os hayan resultado interesantes así como prácticos estos dos artículos.

Aunque en este caso la red inalámbrica a instalar y configurar tenía que tener unas determinadas características impuestas anteriormente, nos puede resultar muy interesante a la hora de diseñar una red inalámbrica con otras características. Hay cosas que no cambian.



Determinar el material inalámbrico es muy importante, aunque a veces, como fue en este, caso hay que adaptarse al material disponible y arreglárselas como se pueda.

DETERMINAR EL MATERIAL INALÁMBRICO ES MUY IMPORTANTE, AUNQUE A VECES, COMO FUE EN ESTE, CASO HAY QUE ADAPTARSE AL MATERIAL DISPONIBLE Y ARREGLÁRSELAS



Yo siempre recomiėndo el Router Linksys WRT54G en cualquiera de sus versiones... La opción de poder instalarle un Sistema Operativo GNU/LiNUX nos da mucho juego y muchas posibilidades donde las haya.

Más adelante, quizás cuando acabemos con el tema de la inyección para la ruptura del protocolo de cifrado WEP tocaremos un diseño de una red inalámbrica que quizás nos pueda interesar a muchos... Pero ya la presentaremos más adelante, con tiempo.

Por último, recordaros que tenéis a vuestra disposición mi correo electrónico, mi blog () donde voy comentando aspectos interesantes sobre seguridad informática, noticias y comunicados referentes a Hack Wi-Fi. También tienes a tu disposición un foro donde poder postear todas las dudas que te puedan surgir a leer cualquier texto: http://foro.netting.es. A mayores disponéis de mi página WEB personal (http://www.netting.es), aunque está bastante desatendida... El tiempo no da para todo :b

En el próximo número

En el próximo capítulo de Hack Wi-Fi seguiremos donde lo dejamos hace dos artículos, seguiremos con la explicación y práctica de la inyección para la ruptura del protocolo de cifrado WEP. Aun no tengo lo suficiente claro lo que vamos a tocar. Pero seguro que nos resultará lo bastante interesante y práctico.

Un saludo lectores, nos leemos ;)

NeTTinG (Enrique Andrade González)

Dedicado: a Mi padre, a mi madre y a mi hermano.

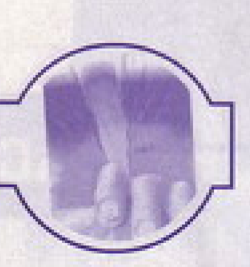
nettinghxc@gmail.com
http://www.wadalbertia.org
http://www.foro.netting.es
http://blog.netting.es



firefox seguro

Blindando nuestro navegador favorito frente a los peligros de la Red

La Red de Redes siempre ha sido un territorio con cierto carácter ambiguo, gris, casi anárquico. Los propios ideales con los que fue concebida la tecnología que ha dado lugar a la revolución de la Web son, en gran parte, los responsables de este carácter de arma de doble filo: tremendamente útil y, si no se va con cuidado, alarmantemente peligrosa. Se está volviendo tristemente habitual el hecho de encontrarse noticias sobre nuevas e inquietantes vulnerabilidades, páginas maliciosas, estafas online, intentos masivos de phising... y, ¿qué podemos hacer nosotros? ¿Acaso estamos indefensos ante estas vicisitudes? Por suerte para nosotros, no es el caso. Veamos cómo podemos defendernos.



Hola a todos una vez más, pasad y poneos cómodos. En el presente artículo, y usando el navegador web Mozilla Firefox -una de las mayores revoluciones en el terreno Web de los últimos años-, vamos a realizar un cursillo acelerado para terminar obteniendo un navegador web blindado. ¿Te interesa, verdad? Pues sigue leyendo...

Eligiendo el navegador

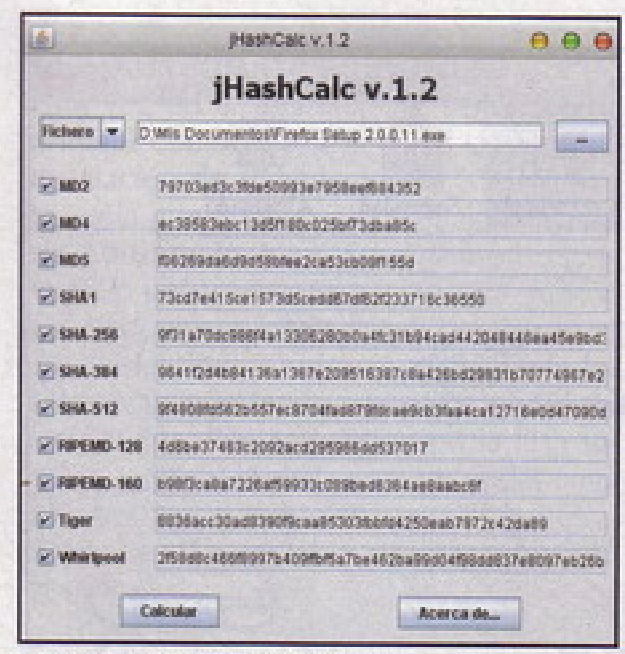
Como ya he comentado, el navegador web seleccionado para el desarrollo del presente texto será Mozilla Firefox. Un servidor ya era usuario de Mozilla bastante antes del nacimiento, bajo el nombre de Mozilla Phoenix, del niño mimado de la Fundación Mozilla. Prácticamente tras su liberación, comencé a usarlo como navegador habitual, y así he continuado haciéndolo hasta la fecha, habiendo visto pasar sus distintas denominaciones (Phoenix, Firebird, Firefox, e Iceweasel en Debian), así como infinidad de versiones.

Existen otros navegadores a los que tengo en alta estima, como Opera, Konqueror o Epiphany. Pero, por diversos motivos, no están, en mi humilde opinión, a la misma altura que Firefox: Opera no es software libre, aunque sí gratuito y multiplataforma (lo uso hasta en mi teléfono móvil y mi Wii); Konqueror me resulta bastante aparatoso, a pesar de su integración en el escritorio KDE; y Epiphany es, en mi opinión, insulso hasta el tedio (lo siento, gnomeros :-P). Obviamente, y creo que no hará falta extenderme en explicaciones, Internet Explorer jamás fue una opción a considerar: puede que unos me gusten más y otros menos, pero sólo tomo en consideración los navegadores serios.

Así pues, una vez elegido el navegador, queda seleccionar la plataforma sobre la que lo ejecutaremos. Sólo podía elegir entre un entorno Unix (por ejemplo, GNU/Linux) o Windows, y a pesar de mis preferencias personales, he decidido que utilizaremos el segundo. El principal motivo es que el proceso es prácticamente idéntico en ambos sistemas, y creo que a los usuarios de sistemas tipo Unix les resultará más sencillo modificar las dos o tres cosas que pueden resultar diferentes.

Descargando e instalando Firefox

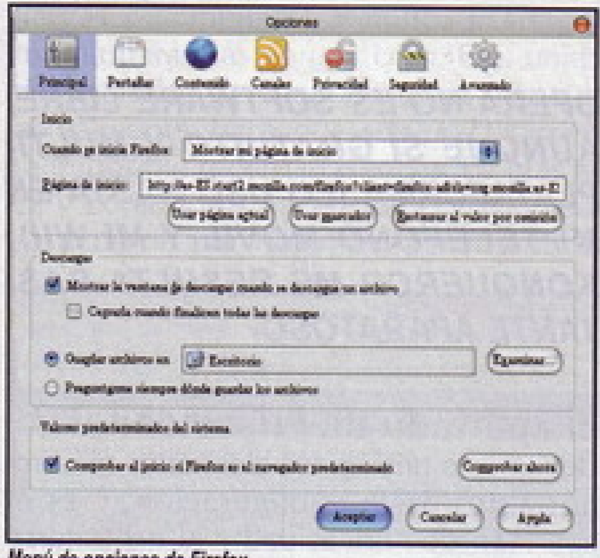
Una vez hemos tomado todas las decisiones necesarias, ha llegado el momento de descargar e instalar el software. Para ello, iremos a la página web europea de la fundación Mozilla que aloja las descargas del navegador: http://www.mozilla-europe.org/es/products/firefox/. En la portada veremos un enlace para descargar el instalador de la última versión del navegador ya en castellano (pues autodetecta la configuración del idioma del navegador), la 2.0.0.11 en el momento de escribir estas líneas.



Comprobando la integridad del instalador



Aspecto del navegador tras su instalación



Menú de opciones de Firefox

Una vez descargado, conviene comprobar la integridad del fichero, para lo cual comprobaremos que el tamaño (5.820.304 bytes), así como los hashes MD5 (f06269da6d9d58bfee2ca53cb09f155d) y SHA-1 (73cd7e415ce1573d5cedd67df62f233716c36550) concuerdan.

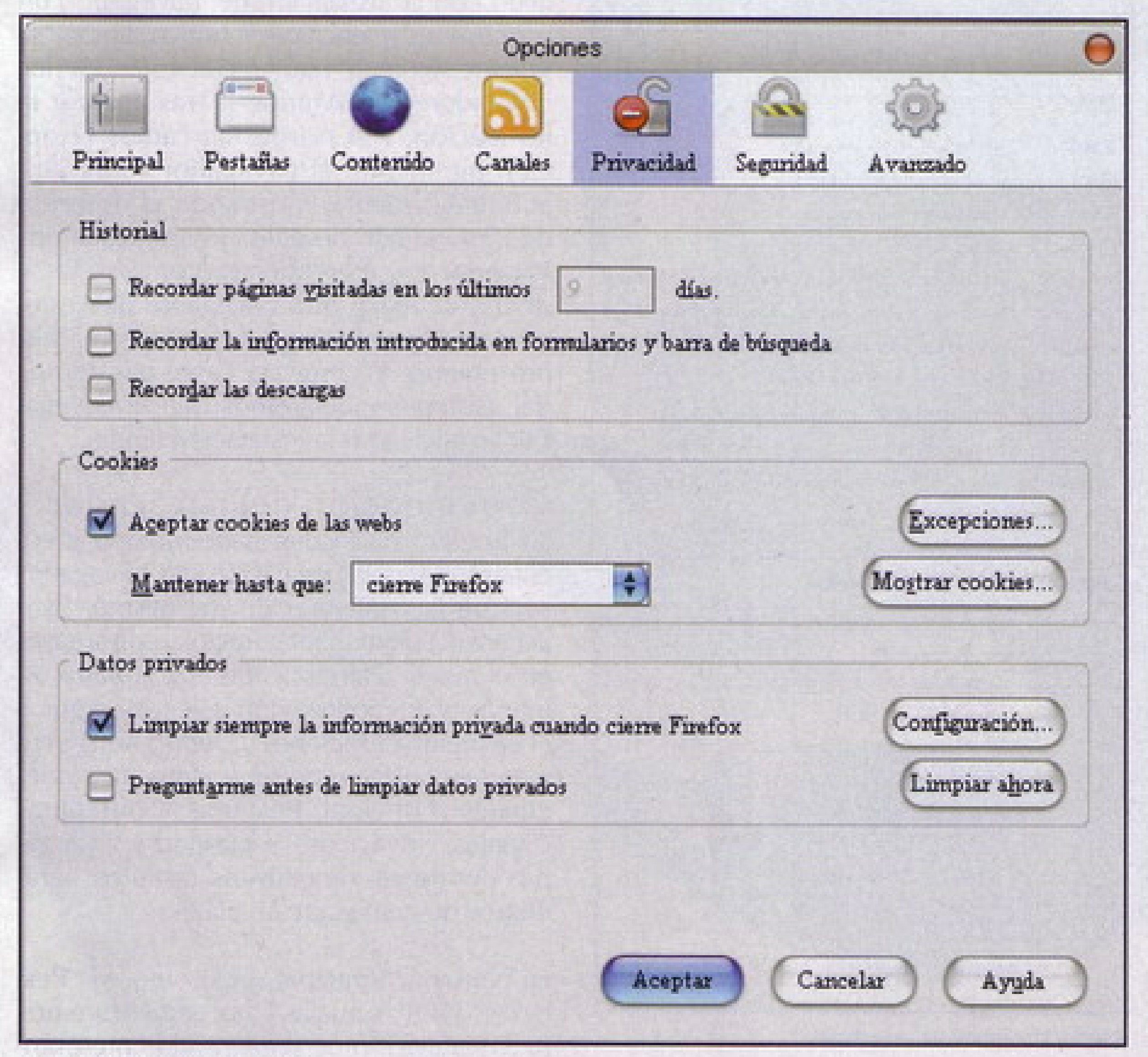
Ha llegado el momento de meternos de lleno con la instalación del navegador, un proceso muy sencillo e intuitivo, típico "siguiente-siguiente-siguiente-aceptar" de los instaladores de Windows. Tras finalizar la instalación, y si no desmarcamos la opción pertinente, el navegador se iniciará automáticamente, mostrando el asistente de importación de datos por si deseamos importar los marcadores, contraseñas y demás de algún otro navegador que estuviéramos usando anteriormente en el mismo equipo. En nuestro caso, pasaremos del asistente y dejaremos que el navegador se inicie con la instalación limpia.

Configuración del navegador

Lo primero de lo que habremos de preocuparnos tras la instalación del navegador será de la configuración del mismo. Para acceder a dicha configuración, pulsaremos en el menú "Herramientas" de la barra de menús, y a continuación seleccionaremos el elemento "Opciones". Dentro de la ventana, encontraremos siete elementos principales (Principal, Pestañas, Contenido, Canales, Privacidad, Seguridad y Avanzado) donde se agrupan los distintos parámetros de configuración afines.

En el menú "Principal", así como en "Pestañas" y en "Canales", no encontraremos ninguna opción que nos resulte interesante para la temática abordada por este artículo, así que cada cual es libre de configurar sus elementos conforme a sus preferencias personales. El menú de "Contenido" sí tiene ciertos elementos que merece la pena, como mínimo, comentar. En primer lugar tenemos la opción de bloquear ventanas emergentes, activada por defecto. Esta configuración se basa en el método de la "lista blanca", mucho más restrictivo que el método complementario (la "lista negra"), pues bloqueará por defecto todos los sitios que traten de lanzar ventanas no solicitadas -y algunas sí solicitadas- mientras no sea indicado explícitamente lo contrario en la lista de sitios permitidos.

La opción de cargar imágenes automáticamente, por contra, tiene un comportamiento por defecto opuesto al de las ventanas emergentes: cargará las imágenes de cualquier sitio web, a no ser que sea bloqueado incluyendo el sitio en la lista de restringidos. Es posible, no obstante, invertir este comportamiento desmarcando la casilla y generando una lista blanca; lo cual, si bien más seguro, es tremendamente incómodo a la hora de navegar: cualquier página se mostrará sin imágenes, y habrá que ir, una a una, añadiéndolas. En aras de la comodidad, mantendremos el comportamiento por defecto.



Configuración de privacidad de Firefox

Llegamos a una opción interesante, ya que es fuente de un constante chorreo de vulnerabilidades: el código Javascript. Gracias al código Javascript, las páginas pueden presentar comportamientos más avanzados que en el caso de contar únicamente con HTML, además de permitir en ciertas circunstancias descargar de trabajo al servidor Web para delegarlo en el cliente. Esto último es debido a que el código Javascript se ejecuta en el cliente, lo cual tiene una serie de implicaciones bastante interesantes en el ámbito de la seguridad: desde las vulnerabilidades que puede suponer si no se trata con cuidado, como robo de cookies; hasta el entretenimiento (y potencial ahorro) que puede proporcionar cuando una página web está mal diseñada, como ciertas páginas de compra online... eso me han dicho, claro, yo no sé nada de esto... :-P

Precisamente la importancia de este tipo de código hará que lo tratemos de una forma especial, a través de un complemento del navegador del que hablaremos dentro de un rato. Por el momento, podemos dejar la configuración tal y como está.

OPERA NO ES SOFTWARE LIBRE, AUNQUE SÍ GRATUITO Y MULTIPLATAFORMA (LO USO HASTA EN MI TELÉFONO MÓVIL Y MI WII); KONQUEROR ME RESULTA BASTANTE APARATOSO

El apartado de Privacidad

Llegamos a uno de los elementos más importantes de la configuración, y es el apartado de "Privacidad". Al no tratarse de contraseñas propiamente dichas, mucha gente considera erróneamente que este apartado no es importante. ¿Puede ser importante o sensible el historial, las descargas o las cookies? Pues me temo que sí.

Para empezar, deshabilitaremos la opción de recordar el historial de navegación. ¿Que quieres recordar una dirección determinada? Pues para eso están los marcadores. Puede parecer una tontería, pero la lista de todas las páginas que ha visitado una persona a lo largo de una semana, puede suponer una cantidad de información bastante respetable. Claro está, este punto puede flexibilizarse bastante según la finalidad del equipo en que hayamos instalado el navegador: personalmente, en el sobremesa de mi casa sí que almaceno el historial de navegación de una semana, mientras que en el portátil almaceno el historial diario, y en el ordenador del trabajo no almaceno absolutamente nada.

También desactivaremos la opción de recordar la información introducida en formularios y la barra de búsqueda. Francamente, nunca he terminado de encontrar la utilidad de esta opción, salvo para casos muy particulares. En la mayoría de los casos, los formularios contendrán información personal que recordamos perfectamente, y que no conviene que almacenemos en el ordenador de forma gratuita. La opción de recordar descargas también debería deshabilitarse, por el mismo motivo que el historial.

Galletitas...

Llegamos al apartado de las cookies, uno muy interesante. A grandes rasgos, las cookies son una "chapucilla" que se inventó para dotar al protocolo HTTP (HyperText Transfer Protocol), un protocolo sin estado, de características que permitieran simular conexiones con estado. Bien usadas, permiten a un determinado servidor web almacenar una pequeña cantidad de información en el ordenador con el cliente (el navegador web), que podrá ser recuperada más adelante por ese mismo servidor (y no otro).

Como siempre, hecha la ley hecha la trampa, veamos un ejemplo. Supongo que casi todo el mundo conoce el archiconocido sistema de foros phpBB, y que lo ha utilizado en alguna ocasión. A la hora de conectarse al foro, si se selecciona la opción de "Conectarme automáticamente en cada visita", se generará una cookie en nuestro navegador, de forma que cuando volvamos a acceder al sitio, la cookie será leída y no será necesario volver a introducir el nombre de usuario y la contraseña. Muy sencillo y muy bonito, pero cuando entra el juego el robo de cookies, bien sea debido a una vulnerabilidad o a pura ingeniería social, nos puede salir el tiro por la culata. En dicha cookie hay almacenada información sensible como el hash de la contraseña, que podría comprometer la cuenta sin siquiera la necesidad de crackearlo.

Luego está la cuestión de la privacidad. Está claro que, en condiciones normales, una cookie sólo puede ser leída por el sitio que la originó. Pero ya sabemos que la publicidad en Internet está más o menos

monopolizada por una serie de sitios encargados de poblar toda página que visitemos de banners (como doubleclick). Si frecuentáis páginas de descargas de contenidos en redes de pares, sabréis a qué me refiero ;-).

La privacidad importa

Pongamos que el dominio cotillas.net se encarga de sembrar la Red de publicidad con sus banners de señoritas ligeras de ropa y casinos online. Nosotros visitamos una página de descarga de películas o de música, y se carga un banner de cotillas.net, que almacena una cookie en la que pone "este tío está visitando lamulamola.org". Después visitamos una página del apasionante mundo de la sexación del ornitorrinco siamés, y se carga otro banner de cotillas.net, que modifica la cookie para añadir "este tío está visitando ornitorrincossiameses.net". Después visitamos una página de... ¿se va pillando el concepto, no? Cumpliendo las normas de las cookies, la gente de cotillas.net está obteniendo nuestro perfil de navegación, de forma que personaliza nuestra publicidad para que veamos muchos banners de p2p o de ornitorrincos. Y, por si alguien se lo está preguntando, sí, ése es el motivo de que haya tantas señoritas liberales en la publicidad de las páginas que soléis visitar. :-P

Sabiendo esto, propongo un par de maneras para tratar las cookies, según el ámbito en el que usemos el navegador. Si el ordenador es privado, y no deseáis perder todos vuestros datos cuando cerréis el navegador, mi recomendación es desactivar la casilla de aceptación de cookies y configurar en "Excepciones" la lista blanca de sitios que tendrán permitida la creación de las mismas en vuestra máquina. En el caso de un ordenador más o menos público, como el del trabajo, recomiendo aceptar todas las cookies, pero que éstas sólo tengan vigencia hasta que se cierre el navegador.

Llegamos a uno de mis apartados favoritos, la limpieza automática de datos privados. Esta característica, que Firefox "tomó prestada" de Opera, es un gran avance en la seguridad del navegador. Básicamente sirve para borrar con un solo click todos los datos que hayamos configurado para ello. Mi recomendación es que esta limpieza se haga de forma automática cada vez que cerremos el navegador, que no pida confirmación, y que se borre todo lo que sea posible. De esta forma, simplemente tendremos que cerrar el navegador para eliminar toda la información privada almacenada en el mismo, y cada ejecución se iniciará totalmente limpia.

El apartado de seguridad

Una vez en el apartado de seguridad, la primera opción interesante es la alerta de instalación de complementos. Obviamente, sería muy mal asunto si cualquier página pudiera instalar complementos en nuestro navegador. Esta restricción funciona mediante el mecanismo de lista blanca, debiendo introducir explícitamente los sitios web que tendrán permitida la instalación. Por defecto, vienen en la lista los sitios "addons.mozilla.org" y "update.mozilla.org", que deberían ser suficientes si no necesitáis instalar alguna extensión "exótica".

La opción de avisar de sitios sospechosos de engaño es interesante, y como tal es bueno tenerla activada, pero no es muy efectiva que digamos. En primer lugar, he visto algunos sitios inofensivos incluidos en la lista negra de Google (entre otras); y en segundo lugar, sólo nos protege de sitios cuyo carácter pernicioso es ya conocido, lo cual no nos ayudará mucho ante vulnerabilidades nuevas. No obstante, como tampoco estorba, la dejaremos activada.

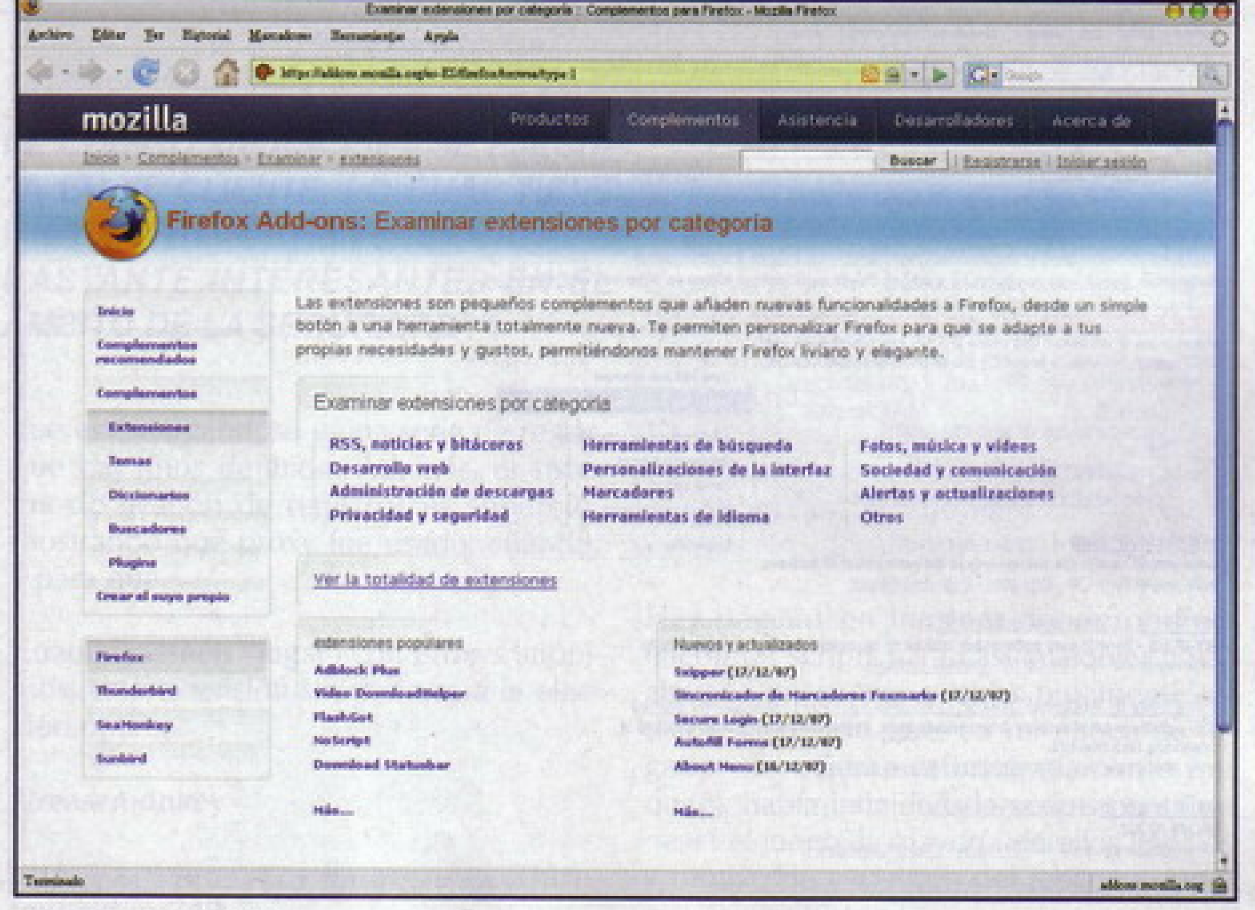
La opción de recordar contraseñas es un poco... delicada. Si sois precavidos con el tema, vuestras contraseñas serán fuertes (largas y complejas), y nunca usaréis la misma para más de una cosa. Eso, unido a la infinidad de cuentas que se manejan actualmente, hace que sea prácticamente imposible recordarlas todas. Lo más fácil y cómodo es hacer que el navegador se acuerde por nosotros, pero también puede resultar muy peligroso en caso de vulnerabilidad. Por ello, lo más recomendable es que el navegador no se utilice para recordar las contraseñas, y, en su lugar, se use para ello algún software de cifrado (como GnuPG o TrueCrypt) que no esté directamente implicado en el proceso de navegación.

Sí es absolutamente imprescindible, en el caso de que decidáis recordar las contraseñas en el navegador, que establezcáis una contraseña maestra, que será requerida por el navegador para desbloquear a las demás. Esto protegerá nuestras contraseñas de "miradas indiscretas" cuando el navegador esté instalado en un equipo con cierto nivel de acceso público.

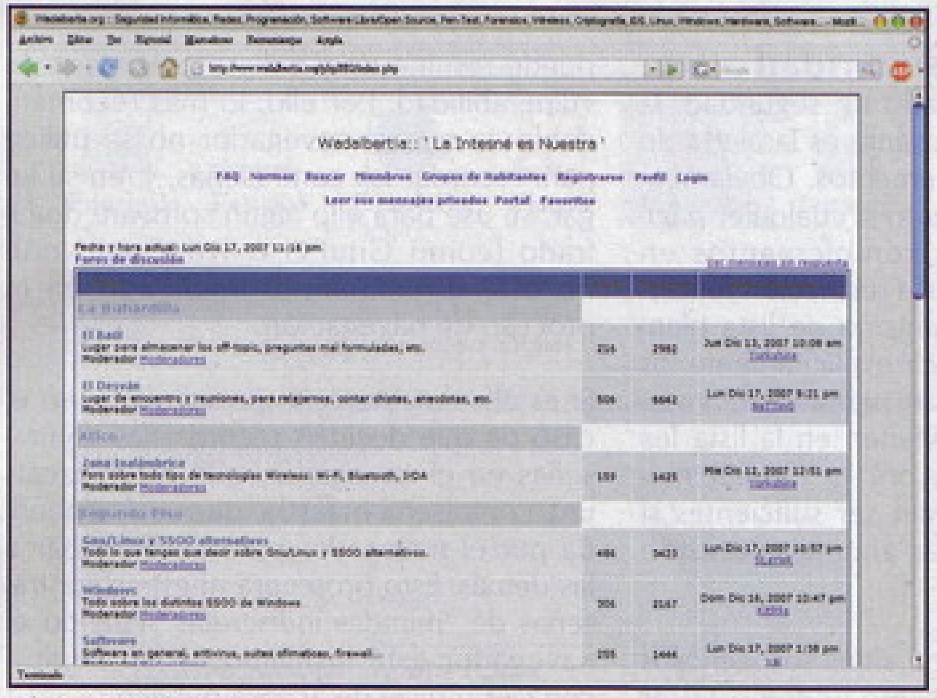
Por último, en el apartado de las advertencias del navegador conviene tener activadas todas las opciones, si bien no es demasiado importante, pues el usuario poco puede hacer salvo no utilizar las páginas que eleven uno de estos mensajes. Además, alguien con los conocimientos necesarios para preocuparse por el nivel de cifrado de una página, no tendrá problema para comprobar estos mismos datos a través del visor de certificados del navegador.

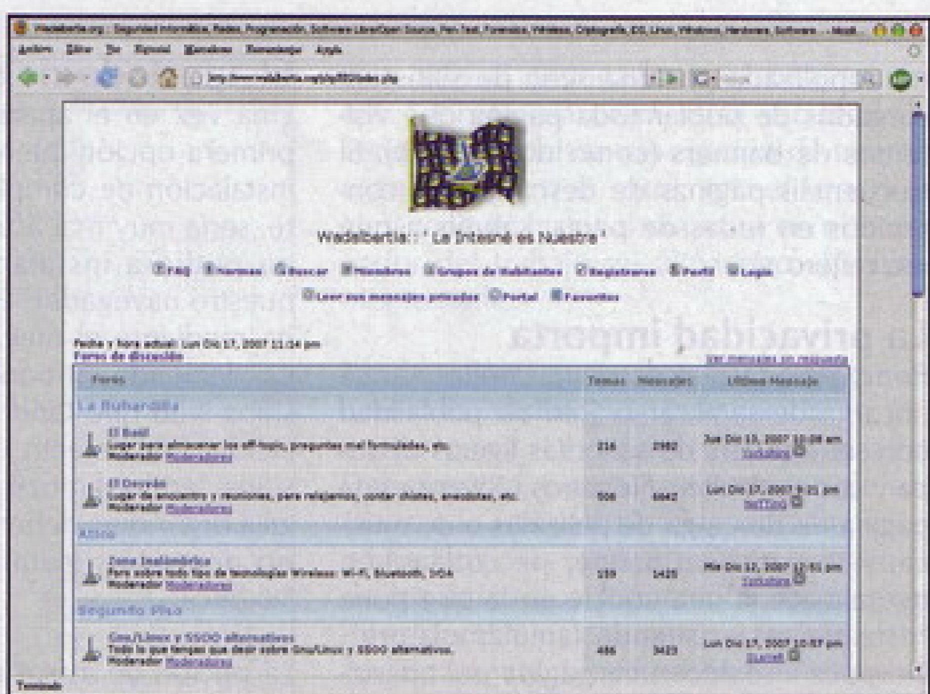
Los complementos

Una de las características estrella del navegador Mozilla Firefox, y que heredó de su antecesor Mozilla, es la capacidad de incorporar extensiones que aumenten o modifiquen su funcionalidad. De esta for-



Sitio de complementos de Mozilla


Página con imágenes bloqueadas


Página sin bloquear imágenes

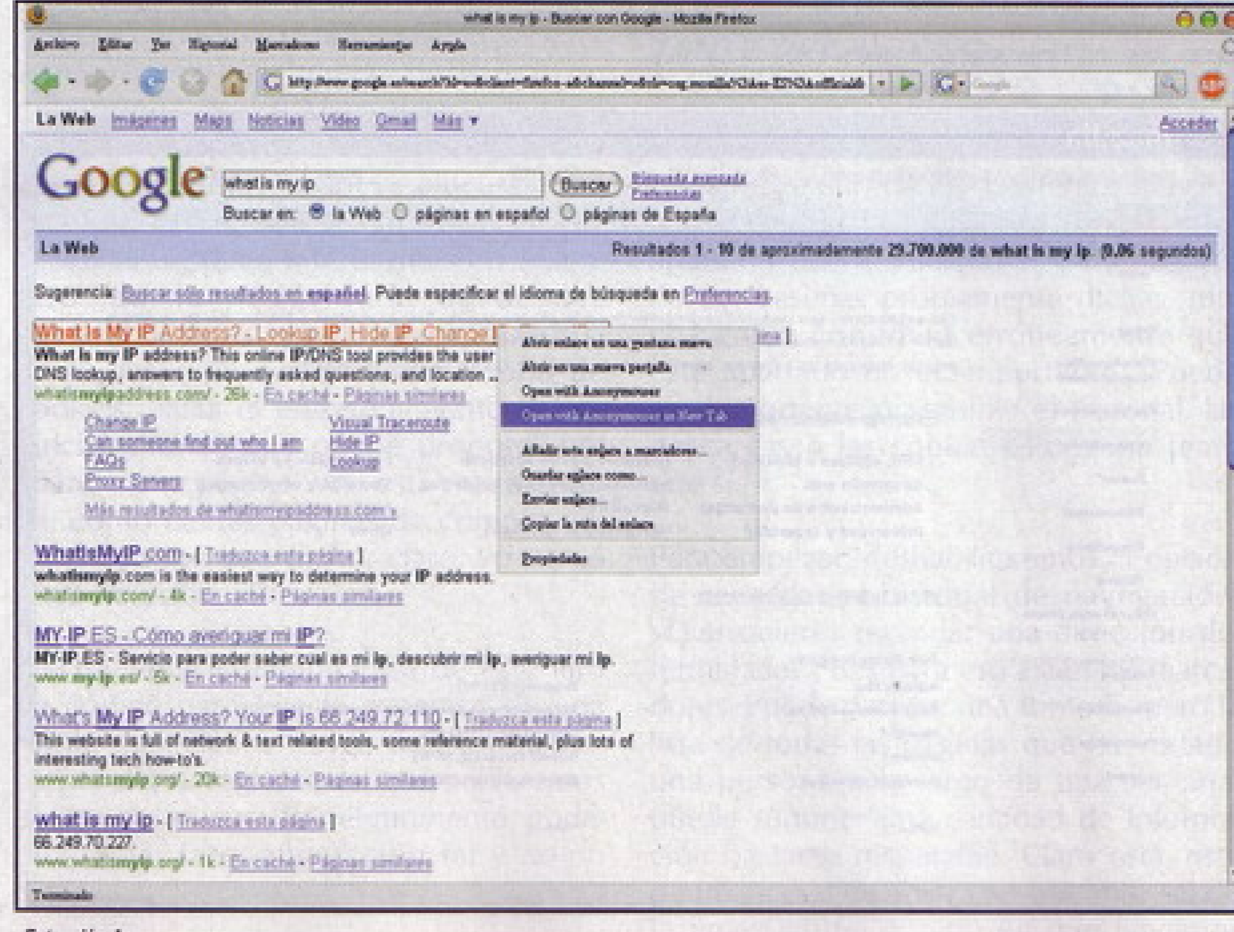
ma, como si de un lego digital se tratase, podemos modificar el navegador para convertirlo en todo aquello que deseemos: un bastión, una herramienta de hacking, un sistema de navegación anónima, una utilidad de desarrollo web...

Estas extensiones, programadas en lenguaje XUL (XML-based User-interface Language), son los pequeños fragmentos de código que nos permitirán llevar a cabo dichas modificaciones. Claro está, un exceso de extensiones hará que el consumo de recursos del navegador se dispare (que me lo digan a mí), pero aquí la idea no es tener un navegador ligero, sino uno seguro. Como dice un buen amigo mío, el kilo de memoria está muy barato. :-)

EL NAVEGADOR SE INICIARÁ AUTOMÁTICAMENTE, MOSTRANDO EL ASISTENTE DE IMPORTACIÓN DE DATOS POR SI DESEAMOS IMPORTAR LOS MARCADORES, CONTRASEÑAS Y DEMÁS DE OTRO NAVEGADOR

En la página de complementos de Mozilla (https://addons.mozilla.org/es-ES/firefox/browse/type:1) podremos encontrar, literalmente, cientos de extensiones diferentes para nuestro navegador, perfectamente categorizadas y clasificadas. Además, el sistema de comentarios y de valoraciones facilita el proceso de selección.

Por supuesto, esta capacidad nos va a permitir modificar nuestro navegador hasta obtener lo que estamos buscando: un Firefox blindado. Así pues, vamos allá con las extensiones.


Extensión Anonymouser

Adblock Plus

https://addons.mozilla.org/es-ES/firefox/addon/1865

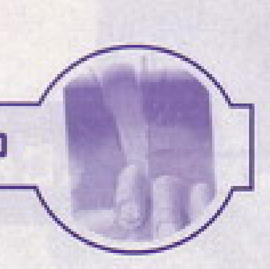
Con esta extensión podemos bloquear esos molestos anuncios que inundan nuestro navegador por doquier. Puede funcionar de forma autónoma, teniendo que indicarle los elementos que deseamos desactivar (elementos concretos o dominios completos), y también mediante la utilización de listas de filtrado ya elaboradas, pudiendo descargar algunas de las muchas existentes en la red, mantenidas por la comunidad, y que contienen ya una gran cantidad de sitios filtrados.

Resulta especialmente interesante si el navegador lo van a usar los más pequeños de la casa, pues ya sabemos el tipo de publicidad que suele dar más dinero a las páginas que desean 'costearse el alojamiento.

Anonymouser

https://addons.mozilla.org/es-ES/firefox/addon/1415

Seguramente algunos de vosotros conoceréis la página anonymouse (http://anonymouse.org/), un auténtico clásico en el tema de navegación anónima. Pues bien, mediante esta extensión podemos abrir enlaces directamente a través de dicha página, de forma que nos redirigirá el enlace a una dirección del estilo de http://anonymouse.org/cgi-bin/anon-www.cgi/dirección_introducida.

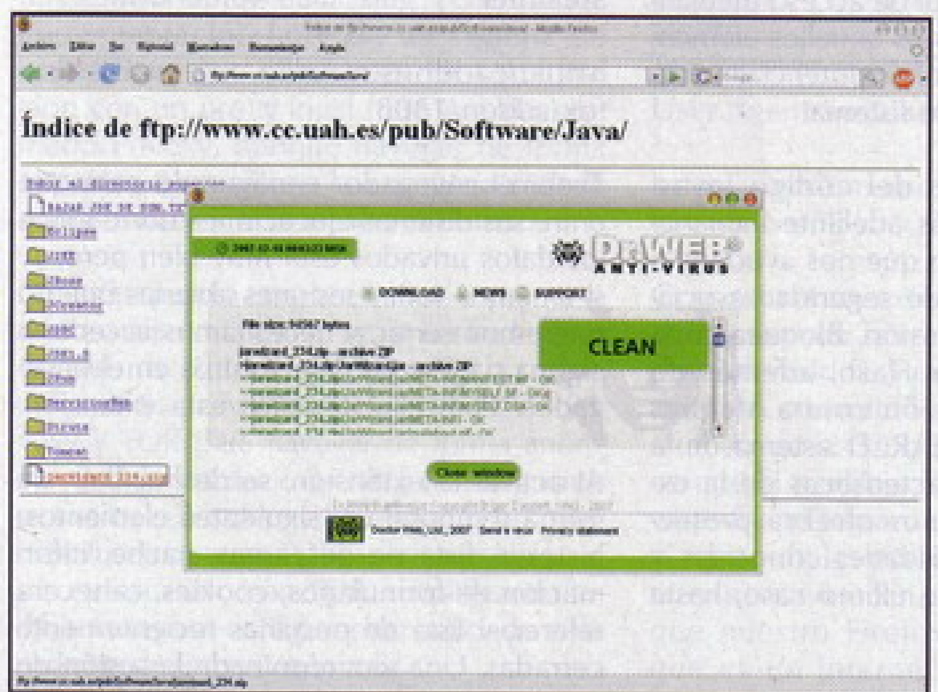


En el menú contextual de navegación se crearán dos nuevas entradas para utilizar la extensión: "Open with Anonymouser" y "Open with Anonymouser in New Tab". Puede resultar útil para consultar una única página sin dejar el rastro de nuestra dirección IP, aunque no es muy cómodo para la navegación anónima. Para eso, hablaremos más adelante de otras extensiones.

Dr.Web anti-virus link checker

https://addons.mozilla.org/en-US/firefox/addon/938

Gracias a esta extensión, muy útil para los usuarios de Windows, podremos escanear en busca de virus cualquier fichero, antes incluso de descargarlo a nuestro disco duro. Para utilizar la extensión, simplemente debemos pulsar con el botón derecho sobre el enlace al fichero, y seleccionar en el menú contextual la opción "Scan with Dr.Web".



Escaneando online un fichero con Dr.Web

Tras pulsar, aparecerá una ventana emergente con un gráfico de espera mientras el fichero es escaneado. Cuando la comprobación termine, se mostrará en la misma ventana un informe pormenorizado del escaneo: estado, tamaño, lista de ficheros (en el caso de tratarse de un fichero comprimido), etc.

Si sois aficionados a descargar todas las tonterías que se envían en los correos en cadena o similares, puede salvaros de algún disgusto...

External IP

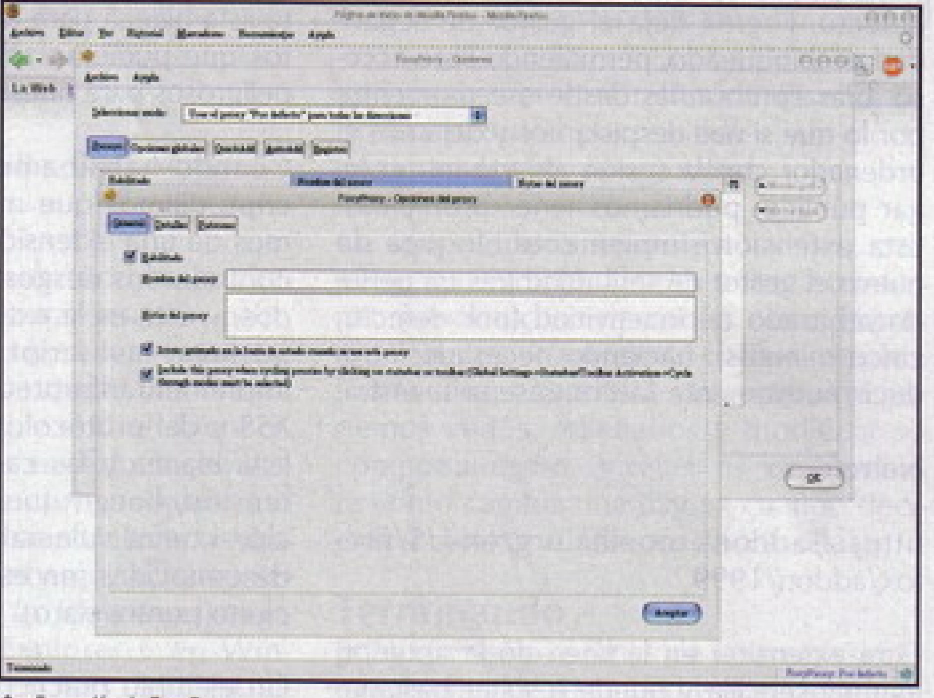
https://addons.mozilla.org/en-US/firefox/addon/3372

Esta sencilla extensión simplemente muestra en la barra de estado la IP externa que está siendo utilizada en nuestra conexión, permitiendo lanzar una alerta cuando dicha dirección cambie. En el caso de equipos portátiles que se muevan por muchas redes diferentes, puede resultar bastante útil.

FoxyProxy

https://addons.mozilla.org/en-US/firefox/addon/2464

Esta extensión es una auténtica maravilla en cuanto al tema de servidores proxy se refiere. Aparte de las típicas opciones para gestionar los diferentes servidores, esta extensión ofrece una serie de particularidades bastante interesantes, como la capacidad de conmutar automáticamente el servidor proxy en uso según la dirección



Configuración de FoxyProxy

EL CÓDIGO JAVASCRIPT SE EJECUTA EN EL CLIENTE, LO CUAL TIENE UNA SERIE DE IMPLICACIONES BASTANTE INTERESANTES EN EL ÁMBITO DE LA SEGURIDAD

que esté cargándose y una serie de reglas que hayamos definido. Además, el sistema de gestión de registros es soberbio, mostrando qué proxy fue usado, cuándo, y para qué.

Cuando deseéis "jugar" con proxys anónimos, esta extensión sin duda será la elección óptima.

Greasemonkey

https://addons.mozilla.org/en-US/firefox/addon/748

Una de mis extensiones favoritas. Su funcionamiento es simple en extremo: permite aplicar un determinado código en Javascript a determinados dominios. Ese sencillo mecanismo permite poner en juego una cantidad casi ilimitada de posibilidades. ¿Recordáis cuando hablábamos de cómo el Javascript era usado en el cliente para modificar las páginas web? Pues ahora podemos hacerlo a nuestro antojo.

Por ejemplo, con un script de apenas cuatro líneas podría eliminarse la publicidad de Google Adsense.

Maquetación: a partir de ahora, denotaré el código fuente (o las órdenes sobre línea de comandos) mediante una tabulación de 1,25 (como esta llamada de atención) y tipografía cursiva, de forma que si deseáis tratar dicho texto de forma diferente, podéis identificarlo fácilmente.

```
var iframes = document.getElementsByTagName("iframe");
for(var x = 0;
x<iframes.length; x++){
    if(iframes[ x] .getAttribute("name") ==
"google_ads_frame")
        iframes[ x] .style.display = "none";
}
```

Hay páginas en Internet donde podréis encontrar scripts para casi cualquier cosa, algunos muy útiles y otros puramente lúdicos. Recuerdo que, en mi época de jugador de oGame (afortunadamente me quité), había infinidad de scripts para "tunear" el juego, la mayoría de ellos ilegales y motivo de expulsión del juego, aunque eso es otra historia...

Master Password Timeout

https://addons.mozilla.org/en-US/firefox/addon/1275

Nos encontramos ante otra extensión increíblemente simple, pero que resulta imprescindible en nuestro Firefox. Cuando hablamos antes de contraseñas, mencionamos la importancia de establecer una contraseña maestra en el navegador, en el caso de que hubiéramos optado por recordar contraseñas en el mismo. Así, cuando accedamos a una página que requiera alguna de las contraseñas almacenadas en el navegador, se solicitará la contraseña maestra para desbloquear el gestor de seguridad.

Pero, ¿qué pasa a partir de entonces? Por defecto, Firefox deja el gestor de seguridad desbloqueado, permitiendo libre acceso a las contraseñas desde ese momento, por lo que si nos despistamos y dejamos el ordenador con la sesión abierta en un lugar público, podríamos tener problemas. Esta extensión simplemente bloquea de nuevo el gestor de seguridad tras un período arbitrario de inactividad (por defecto, cinco minutos), haciendo necesario introducir nuevamente la contraseña maestra.

No-referrer

https://addons.mozilla.org/en-US/firefox/addon/1999

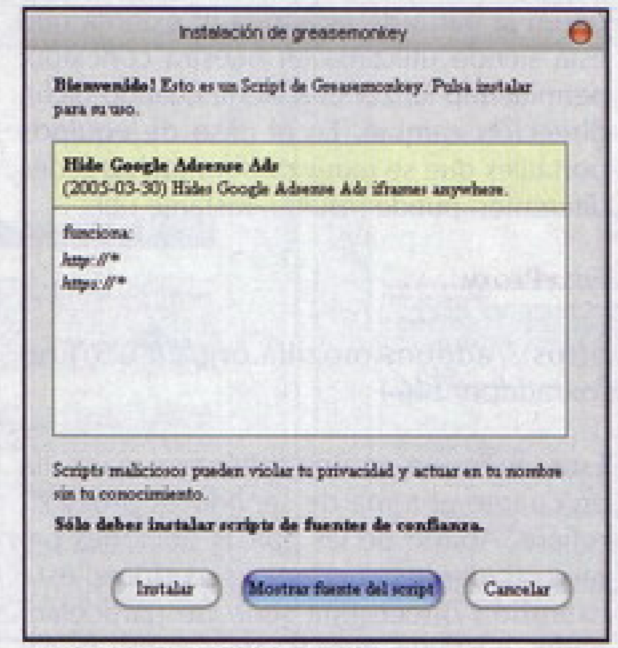
Otra extensión en la línea de la anterior, es muy sencilla y puede resultar bastante útil. Simplemente añade al menú contextual de navegación una nueva opción etiquetada como "Open link in New Tab Without Referer", que nos servirá para acceder al enlace pulsado, pero sin enviar la información sobre el referer del que proviene la visita.

Si queréis, por ejemplo, acceder a una página encontrada en un buscador, pero sin dejar rastros de la cadena de búsqueda introducida en el mismo para llegar hasta ella, ésta extensión es lo que necesitáis.

NoScript

https://addons.mozilla.org/en-US/firefox/addon/722

Llegamos a la que es, muy posiblemente, la extensión de seguridad por excelencia para Mozilla Firefox. De hecho, dentro de la categoría de privacidad y seguridad de las extensiones, es la primera en populari-



Instalación de un script de Greasemonkey

dad. Su funcionamiento básico consiste en implementar un control de acceso mediante lista blanca para todos aquellos elementos que pudieran resultar potencialmente peligrosos para nuestro sistema.

Cuando hablábamos del código Javascript, dijimos que más adelante hablaríamos de una extensión que nos ayudaría a controlar los riesgos de seguridad asociados, y ésta es la extensión. Bloquea código Java, Javascript y Flash, además de implementar protección contra ataques XSS y del protocolo JAR. El sistema de la lista blanca y las características de la extensión, hacen que nos ofrezca protección contra vulnerabilidades conocidas y desconocidas (en este último caso, hasta cierto punto, claro).

Un ejemplo práctico pudimos verlo hace poco (en el momento de escribir estas líneas, casi dos meses antes de que lo estés leyendo), cuando un fallo en el protocolo JAR puso en jaque la seguridad del navegador Firefox. Hasta que se publicó la nueva versión corrigiéndolo, la manera más eficiente de protegerse era usar esta extensión. En el caso de que alguien no se hubiera enterado de dicha vulnerabilidad, si hubiera usado NoScript, habría estado protegido aún sin saberlo, mientras que en otro caso habría quedado expuesto durante las casi dos semanas que tardó en corregirse el fallo.

SecurePassword Generator

https://addons.mozilla.org/en-US/firefox/addon/135

Antes, cuando hablábamos de las contraseñas, recordaba la importancia de la fortaleza de éstas. Nadie está libre de que el hash de su contraseña se vea comprometido por cualquier motivo, y una contraseña de seis letras es doblegada por cualquier crackeador de contraseñas en apenas unos minutos. Sin embargo, una buena contraseña alfanumérica con símbolos de doce o más caracteres, llevará su tiempecito el romperla, al menos a nivel doméstico.

Y claro, el problema de siempre es cómo generar estas contraseñas de forma aleatoria o pseudoaleatoria. Esta extensión se encarga de solucionar dicho problema, implementando un método pseudoaleatorio para realizarlo, atendiendo a una serie de parámetros que debemos configurar, como el alfabeto y la frecuencia de caracteres a utilizar.

Stealther

https://addons.mozilla.org/en-US/firefox/addon/1306

Tener el navegador configurado para que entre sus distintas ejecuciones borre todos los datos privados está muy bien pero, ¿y si tenemos varias sesiones abiertas que no queremos cerrar, y necesitamos acceder a alguna página sin dejar rastros en el navegador? Para ello tenemos esta extensión.

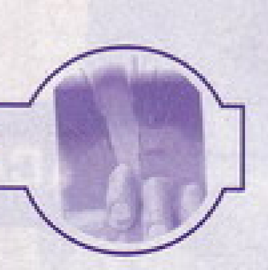
Al activar la extensión, se deshabilitan de forma temporal los siguientes elementos: historial, lista de descargas, caché, información de formularios, cookies, cabecera referer, y lista de pestañas recientemente cerradas. Una vez terminada la sesión de navegación "sospechosa", se desactiva la extensión y se continúa con la sesión que había sin que queden rastros de ese breve (o no) lapso de tiempo.

Tamper Data

https://addons.mozilla.org/en-US/firefox/addon/966

Esta extensión es una especie de "mini sniffer" para HTTP/HTTPS empotrado en Firefox. Permite ver y modificar al vuelo cabeceras y parámetros post de dichos protocolos, de forma que pueden alterarse las peticiones lanzadas al servidor remoto.

Tradicionalmente, para realizar estas operaciones era necesario interponer un servidor proxy en la conexión (recuerdo cierta prueba del reto de hacking izhal) que capturara y retuviera los datos. Tras las modificaciones pertinentes, la información cambiada era lanzada al servidor remoto. Con esta extensión podemos



realizar lo mismo, pero sin la necesidad de interponer un proxy completo y tener que lidiar con su complejo mecanismo.

Y que conste que no sólo de hacking vive el hombre, que esto también puede resultar muy útil á la hora de desarrollar, pues para probar sistemas de petición SOAP a través de un navegador, por ejemplo, puede resultar muy útil.

Torbutton

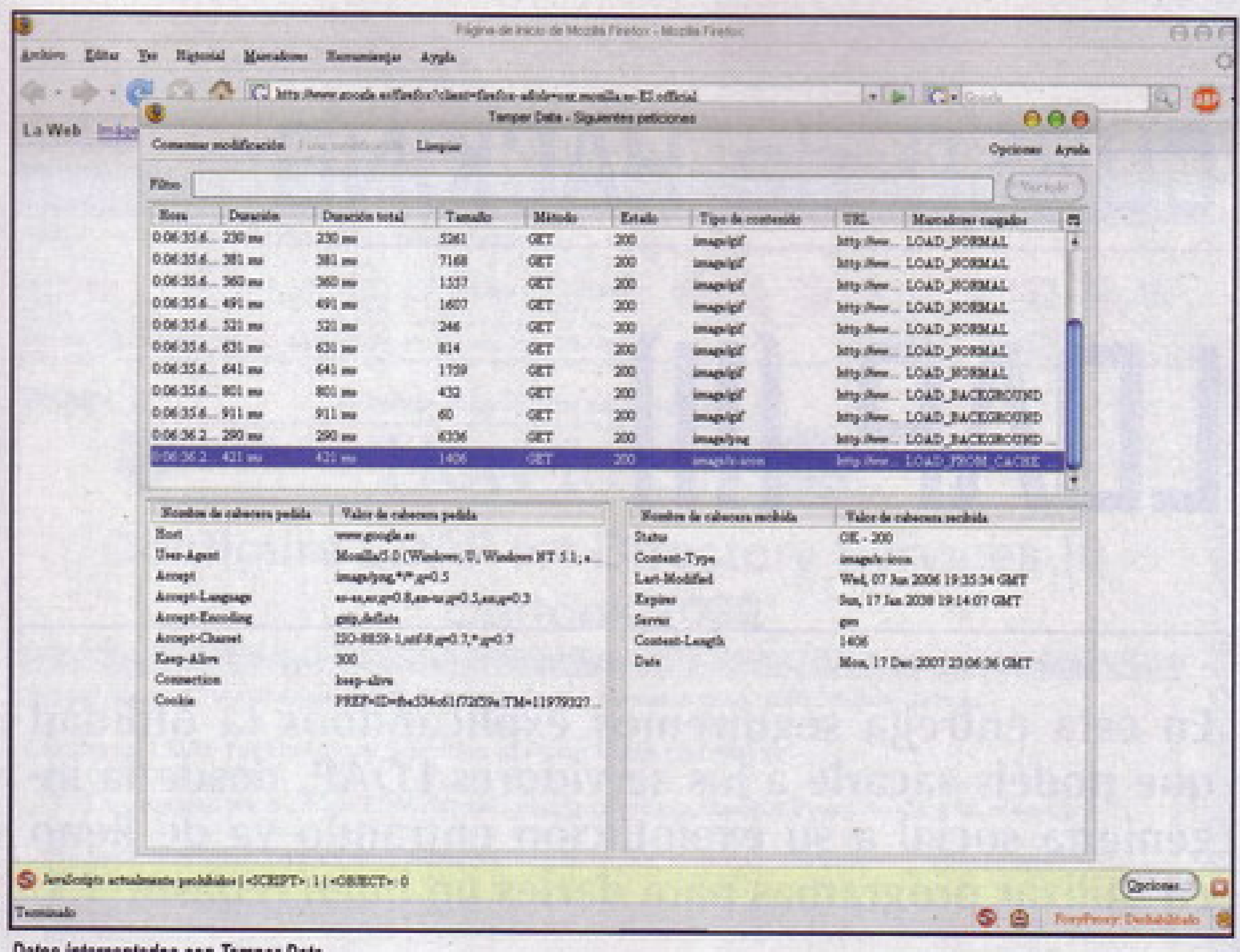
https://addons.mozilla.org/en-US/firefox/addon/2275

Apostaría a que la mayoría de vosotros ha oído hablar alguna vez de TOR (The Onion Router). Como versión muy resumida, podríamos decir que TOR es una implementación libre de un sistema de encaminamiento anónimo. En combinación con un proxy local (tipo Achilles) llamado Privoxy, permite navegar de forma anónima a través de la compleja red de nodos entretejida por todo el mundo.

Como su propio nombre indica, esta extensión instala un "botón" en la barra de estado del navegador que permite, con un único click, activar la salida a través de Privoxy y TOR para navegar de forma anónima. Podríamos decir que su funcionamiento es similar a FoxyProxy (que, de hecho, también funciona con TOR), pero creado para su uso exclusivo con TOR, simplificando toda la farragosa configuración asociada a las cadenas de proxys anónimos.

Una última cosa: ¡ojo con TOR! Es una red anónima, lo cual no quiere decir que sea absolutamente segura. De hecho, yo daría por hecho que todo aquello que no viaje cifrado (a través de SSL o TLS) está siendo cotilleado por medio mundo. Hace poco se publicó la noticia de que un hacker se había hecho con cientos de contraseñas de diplomáticos y políticos de todo el mundo, lo cual causó no poco revuelo en la red y fuera de ella.

Lo único que hizo este hombre fue instalarse un nodo de TOR, ponerse a capturar el tráfico que pasaba por su máquina con un sniffer, y sentarse a esperar a que las contraseñas llegaran solas. Y pudo hacerlo porque mucha gente creía saber cómo funcionaba TOR, pero en realidad no lo sabían: conectaban TOR y navegaban directamente como si tal cosa, pensando que estaban totalmente seguros. Así que ya sabéis: ojo con vuestras contraseñas cuando pasan por algún proxy...



Datos interceptados con Tamper Data

User Agent Switcher

https://addons.mozilla.org/en-US/firefox/addon/59

Gracias a esta extensión podremos "camuflarnos" en la red para pasar un poco desapercibidos. Por ejemplo, si queréis dejar un comentario gastando una broma a un amigo en su blog, y el User Agent dice que el mensaje fue enviado desde Iceweasel en Debian, es muy probable que el rango de las personas sospechosas sea muy pequeño. Sin embargo, si hacemos que nuestro Firefox (o Iceweasel) diga que es un Internet Explorer 6 en Windows XP, pasará mucho más desapercibido, ¿no? Y quien dice dejar comentarios en un blog, dice hacer cualquier tipo de prueba o ataque dejando rastros falsos. Siempre en nuestra propia red, ya sabéis. ;-)

Pues ése es el trabajo que realiza esta extensión: falsea los datos del User Agent enviados por el navegador para hacerse pasar por cualquier combinación de sistema operativo y navegador, real o no.

Web Developer

https://addons.mozilla.org/en-US/firefox/addon/60

Esta extensión, en principio pensada para facilitar la tarea de los desarrolladores web, puede resultar muy, pero que muy interesante en el mundillo de la seguridad informática. Al permitirnos, literalmente, desnudar y modificar la página web hasta sus entrañas, esta extensión nos permite aprovechar ciertos fallos de diseño de programadores poco hábiles y/o poco preocupados por la seguridad.

Os sorprendería saber que existen, por poner un ejemplo, tiendas online en Internet que almacenan variables como el precio en los campos ocultos de los formularios, y gracias a esta extensión podemos verlos, rellenarlos y modificar su comportamiento. A veces es sorprendente cómo cambia una página cuando decidimos mostrar su información oculta...

Terminando

Estas eran sólo algunas de las muchísimas extensiones de seguridad y privacidad que hay disponibles para nuestro navegador favorito. Por supuesto, la seguridad no es algo que deba quedarse en el ámbito del navegador, debiendo existir también un cierto grado de seguridad perimetral, una máquina libre de software malicioso y, por encima de todo, una actitud activa y curiosa por parte del usuario. Toda medida de protección deriva, y puede ser suplida por la actitud de una persona, esa actitud que, a falta de una expresión mejor, denominaremos "espíritu hacker".

Espero que este pequeño texto os haya resultado tan ameno y edificante de leer, como me lo ha resultado a mí de escribir. Tened cuidado ahí fuera, en la Red.

¡Nos leemos!
Dedicado a Abián y Jaime. Dos grandes amigos, dos grandes personas.

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com<



CURSO de HACKING

LDAP (II)

En esta entrega seguiremos explicándoos la utilidad que podéis sacarle a los servidores LDAP, desde la ingeniería social a su explotación entrando ya de lleno en utilizar programas para darles un buen repaso.

Introducción II

Los servidores LDAP almacenan la información en forma de árbol, por lo que para llegar a la información contenida en una hoja tenemos que pasar por las ramas. Cada rama nos da información de las hojas que contiene, por ejemplo, en una organización (raíz del árbol) podemos tener varios departamentos (ramas) y, dentro de cada rama, tenemos a los empleados (hojas) que trabajan en dicho departamento.

Traduciéndolo al lenguaje empleado en LDAP llamaremos a una hoja "entrada". Una entrada puede tener varios "atributos" como serían el nombre, el teléfono, el e-mail... Al final, en un LDAP, todo son entradas con las excepciones de que:

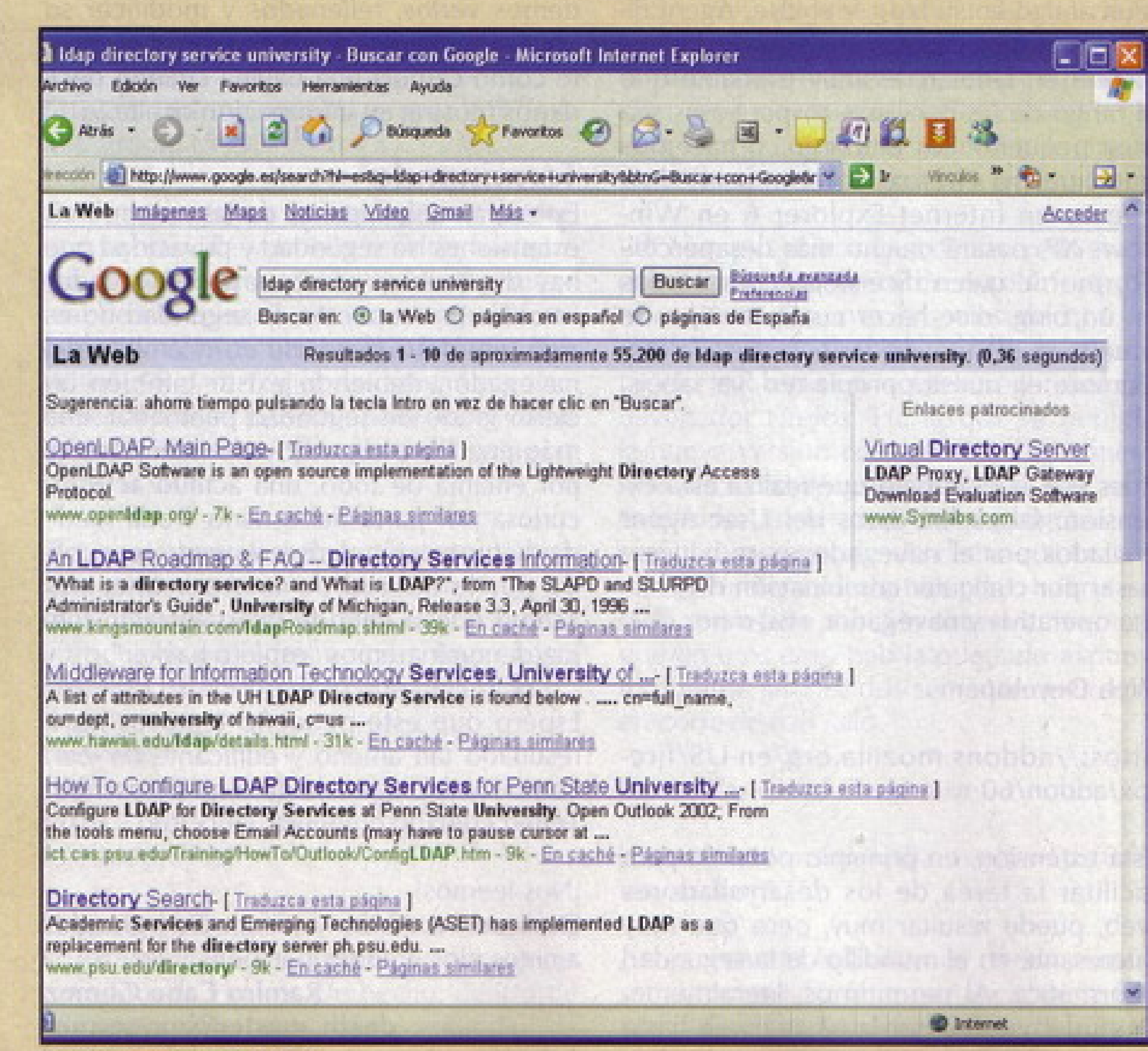
- La raíz es una entrada sin padres y
- Una hoja es una entrada sin hijos

Los atributos se pueden definir como se quieran, es como los datos de las personas que guardamos en las fichas. Por ejemplo, a una empresa le puede interesar poner el atributo "Casado", que indicará "Sí" o "No" según la persona esté casada, para saber si traerá pareja el día de la cena de Navidad. A otras empresas les puede interesar más poner el atributo "AccessLevel" que indica el nivel de acceso que tiene a documentos clasificados. Y así un largo etcétera de atributos que cada empresa va creando según sus necesidades.

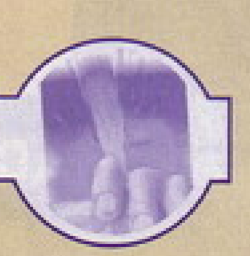
El problema de los atributos es que sólo los entiende quien los ha creado. Por ejemplo, si un empleado tiene en su entrada un AccessLevel 3, nosotros no sabremos eso qué significa (3 puede ser que tenga acceso a todo o que no tenga acceso a nada).

No obstante, hay una serie de atributos que son estándar y que saben interpretarlos cualquier cliente LDAP:

- DC: Domain Component (Componente de Dominio)
- CN: Common Name (Nombre Habitual)
- DN: Distinguished Name (Nombre Distinguido)
- DIT: Directory Information Tree
- OU: Organizational Unit (Departamento)
- C: Country (País)
- RDN: (Nombre Distinguido Relativo)
- ACI: Access Control Instruction (Instrucción de Control de Acceso)



Resultados de la búsqueda de LDAP



Buscando un servidor LDAP con Google

Ya sabéis que no me gusta dar demasiada teoría sin práctica, así que comencemos con la práctica. Vamos a empezar por localizar servidores LDAP con los que empezar a familiarizarnos con el protocolo. Para ello nos iremos a Google y buscaremos:

ldap directory service university

Dado que las universidades tienen a mucho personal (entre profesorado y alumnos), es muy común que dispongan de servidores LDAP para poder localizar el e-mail de los alumnos o los teléfonos de los profesores. Como además suelen estar preparados para poder acceder desde fuera del campus son un buen lugar por donde empezar. Si además lo ponemos en inglés tendremos más posibilidades de encontrar servidores y, además, fuera de nuestro territorio patrio (viajar para nuestra anonimicidad ya sabéis que es bueno jejeje).

Para nuestras pruebas iniciales utilizaremos los datos de este servidor: LDAP.PSU.EDU. Se trata del servidor LDAP de la universidad de Penn State.

Accediendo a un servidor LDAP con Outlook

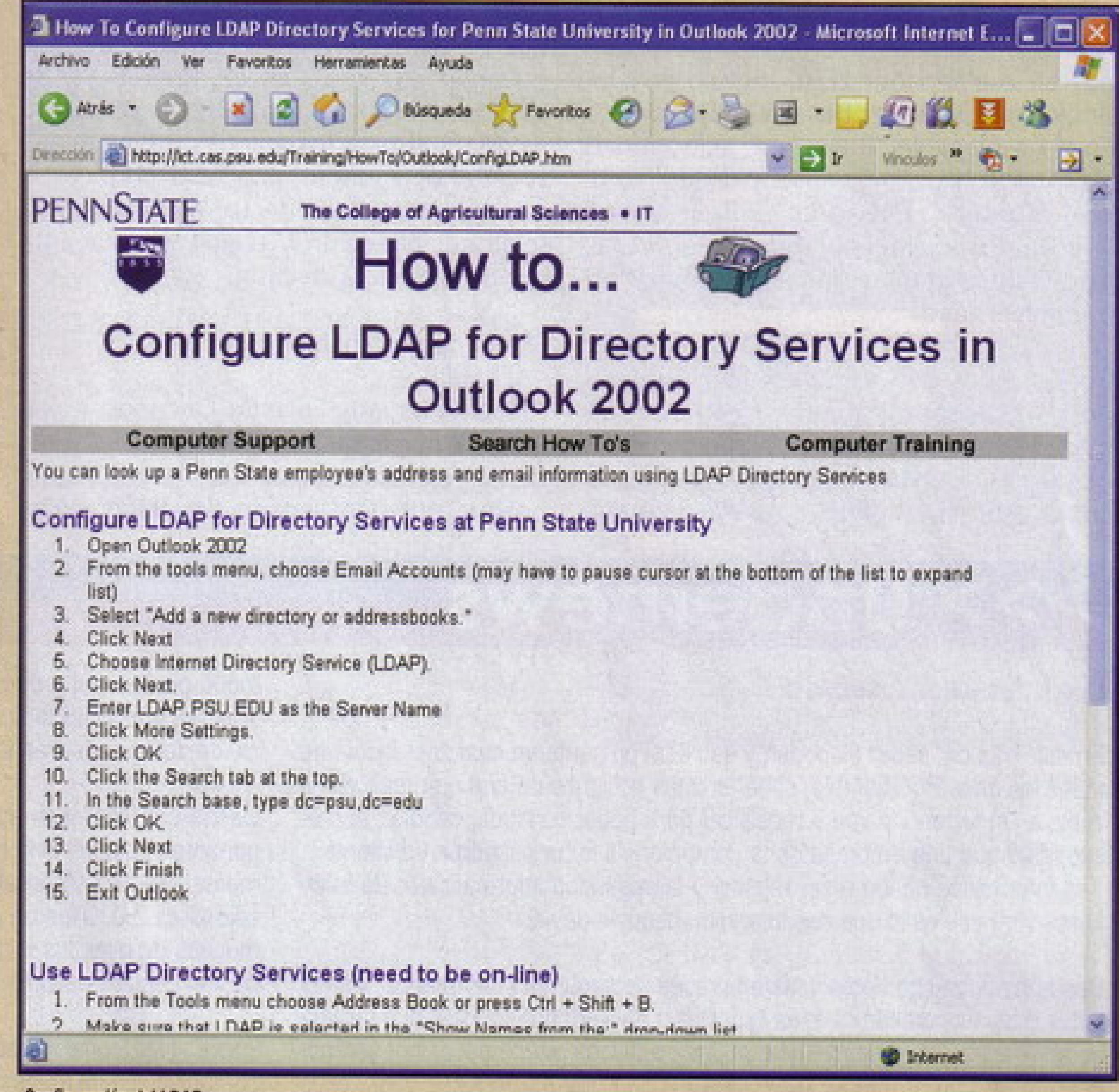
Una de las funciones más habituales de los servidores LDAP es la de proporcionar los datos de contacto de personas, así pues no es de extrañar que los clientes de correo electrónico suelan incorporar un cliente LDAP para poder acceder a estos listados.

Así pues, os vamos a explicar cómo configurar el Outlook Express 6 (que lo tiene cualquiera con Windows) para usarlo como vuestro primer cliente LDAP.

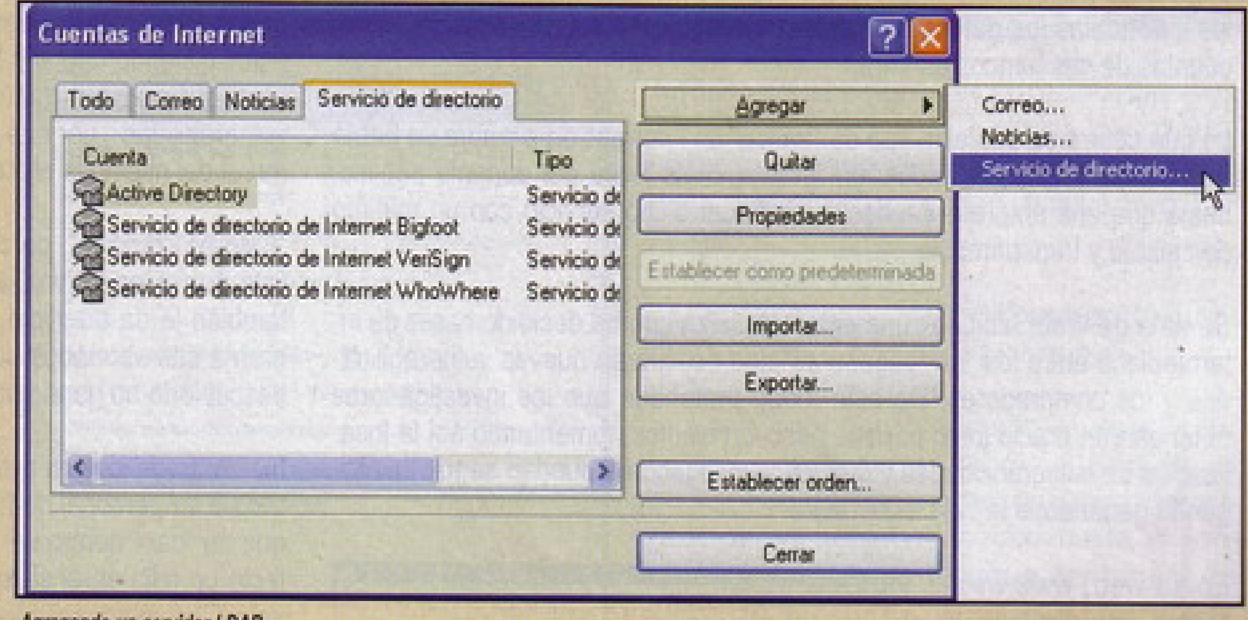
Pulsad en Herramientas ➠ Cuentas... ➠ Agregar ➠ Servicio de directorio...

Ahora introducís en "Servidor de directorio de Internet (LDAP)" LDAP.PSU.EDU.

Pasáis a la siguiente pantalla y a la pregunta "¿Desea comprobar direcciones usando este servicio de directorio?" será mejor que le respondáis que no, si no cada vez que vayáis a mandar un correo a vuestro amigo "Pepe" buscará a ver si hay alguien llamado "Pepe" en esa universidad. Pasáis a la siguiente pantalla y finalizáis la configuración. Ahora seleccionad el servidor "LDAP.PSU.EDU" y pulsad en Propiedades ➠ Opciones avanzadas. Donde aparece "Base de búsqueda" introducid:



Configuración del LDAP



Agregando un servidor LDAP

```
dc=psu,dc=edu
```

Esto último que hemos hecho es especificarle al Outlook que cuando busque a alguien dentro de ese LDAP, que lo haga mirando en las ramas psu y edu.

Aceptad, cerráis el listado de cuentas del Outlook y listo.

El esquema de un LDAP

El esquema de un LDAP solía tener como raíz una entrada con un atributo C indicando el país, pero ya no suele usarse y se ha sustituido por un DC. En el ejemplo que estamos viendo, el DC sería "edu", que sería el raíz del dominio. A continuación, como el dominio son dos palabras, vendría otro DC que sería "psu".

Buscando por un LDAP

Ahora, si queréis buscar datos de personas en ese servidor LDAP pulsad en Outlook en Edición ➠ Buscar ➠ Personas... En el desplegable "Buscar en" seleccionad "LDAP.PSU.EDU" e introducid en "Nombre" "George". Pulsad en "Buscar ahora" y ¡voilá! Os aparecerán decenas de fichas de personas que se llaman "George" en esa universidad.

Bueno, pues con esta sencilla búsqueda podemos empezar a deducir cómo se forman las direcciones de e-mail del personal de dicha universidad. Una cosa tan inocua como esta ya empieza a revelar información. Eso por no hablar de la información que veréis cuando abráis un contacto (cliqueando dos veces en él). Podréis ver su teléfono, dirección, etc. Esta información es muy útil para los ataques de ingeniería social. Por ejemplo, gracias a conocer el nombre completo de un estudiante, su teléfono, dirección y e-mail, un atacante podría llamarlo a su casa:

- Hola, ¿podría hablar con Peter?
- Al habla.
- Hola Peter, soy Fulanito Decopas, trabajo en Administración en el Campus y necesito revisar tus datos que tenemos aquí porque nos han llegado devueltas varias cartas. ¿Tienes un minuto?
- Sí, claro, no vaya a ser que no me lleguen los papeles de la beca.
- Veamos, ¿tu apellido es Falken y vives en C/Washington, nº 3?
- Correcto.
- El e-mail de contacto que tenemos aquí es peter@psu.edu ¿correcto?
- Sí.
- Bien, ahora me falta que me repitas tu número de cuenta en el banco, porque no me aparece nada aquí.
- Espera que te la digo...

En fin, algo así podría ocurrir. Ya sabéis que una mentira es más creíble entre va-

>>> Undernews

Los bugs salen a subasta

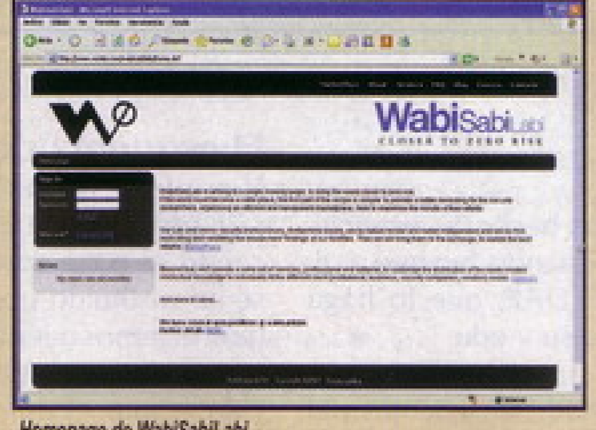
En este mundo, saber es poder, y eso está presente en cualquier faceta de todos los días. Por ejemplo, saber si unas acciones de una empresa van a subir, si un terreno lo van a recalificar para poder construir, conocer el presupuesto que una empresa de la competencia le ha pasado a un cliente... Y la informática no iba a ser menos, y la seguridad informática (o de la información) que es lo que nos interesa, menos todavía.

Desde hace mucho tiempo, las empresas de seguridad informática, los estados o las mafias pagan a los expertos o hackers por conocer nuevas vulnerabilidades. Por ejemplo, una casa de antivirus puede pagar por obtener el software con el que se diseñan a medida hoy día muchos virus, o un grupo mafioso puede pagar por conocer un bug que saca de la caché de los internautas los datos de acceso a las webs (para poder colarse en las cuentas de sus bancos on-line)...

Lo que ocurre es que este tipo de "tráfico" de información siempre se había hecho en círculos reducidos, en foros o chats fuera del dominio público, hasta que una empresa ha decidido ofrecer dicho servicio con un mínimo de calidad y transparencia.

Se trata de WabiSabiLabi, una empresa suiza que ha decidido hacer de intermediario entre los "investigadores" que descubren nuevas vulnerabilidades y los compradores. De este modo pretenden que los investigadores obtengan un precio justo por sus descubrimientos, fomentando así la localización de vulnerabilidades y que los investigadores puedan seguir investigando ganándose la vida legalmente.

En su web, www.wslabi.com, han montado un sistema donde aparecen las vulnerabilidades que ellos mismos han revisado para constatar que son reales, el precio que el investigador pide por ellas y por dónde va la puja... vamos, un eBay pero en chiquitito.



Homepage de WabiSabiLabi

Está claro que este enfoque profesional y de cara al mercado no lo están haciendo por amor al arte, así que WabiSabiLabi se mantiene a base de un porcentaje en el precio de venta de las vulnerabilidades.

Desde que esta web apareció, se abrió un debate sobre si era ético proporcionar este servicio o no. WabiSabiLabi afirma que, de las aproximadamente 139.362 vulnerabilidades que fueron descubiertas el año pasado, sólo unas 7.000 fueron difundidas públicamente, lo que se traduce en que muchas de ellas los investigadores no llegan a publicarlas, o son compradas en círculos oscuros.

Fabricantes como Cisco o Trend Micro no son partidarios de esta salida comercial. En mi modesta y humilde opinión, considero que cada uno es libre de hacer con sus descubrimientos lo que quiera ¿a caso no investigan armas para matar personas los gobiernos, no investigan venenos...? No estoy diciendo que sea lícito, pero lo que no parece correcto es utilizar dos varas de medir. Si un investigador puede ganar dinero por descubrir una vulnerabilidad ¿por qué no va a poder hacerlo? Ya dependerá de la calidad moral del mismo la elección de a quién se lo venderá y a qué precio.

"Esto es como tó", para un experto en seguridad, publicar un bug en una lista de correo le hincha el orgullo, que luego salga publicada en una web también le da prestigio... pero luego se encuentra con empresas que cobran a sus abonados por informarles de esa vulnerabilidad ¡y él que la ha descubierto no gana nada! Eso tampoco es justo.

Me contaron en una ocasión que una empresa de automóviles daba incentivos a su personal de fábrica por detectar defectos en los coches, siempre que no fuera dentro de su sección (por ejemplo, si un técnico eléctrico detecta un fallo en el sistema de amortiguación, la empresa se lo recompensa). ¡Qué mejor manera de que la gente se fije en los detalles y tome el tiempo de informar a la empresa!

Que sería más bonito que la gente lo hiciera gratis, sí, pero a principio de mes llegan las facturas y con una palmadita en la espalda no se pagan... Y si las empresas desarrolladoras (o que monten una web, por poner un ejemplo cualquiera) quieren conocer cuáles son los fallos en su software, que paguen a gente en su plantilla para que audite el código y realice buenas pruebas de calidad, así no tendrán que preocuparse de que sus fallos se vendan al mejor postor. Y si no quieren gastarse dinero en hacer desarrollos de calidad, que no se quejen de que tampoco quieren gastarse dinero en conocer cuáles son sus fallos.



rias verdades, y si no preguntadle a Kevin Mitnick. Moraleja, nunca os fiéis de nadie.

Ya habéis visto lo útil que ha sido esa información que hemos obtenido.

Accediendo a un servidor LDAP con otros clientes

No obstante, hay más información que visualizar, lo que pasa es que el Outlook sólo entiende el contenido estándar de una entrada, y no muestra otra información fuera de lo habitual. Por ese motivo os recomendamos que utilicéis el LDAP Browser/Editor, un programa opensource que os permitirá ver la información del LDAP al completo. Lo tenéis en LDAP Browser-Editor - Browser282b2.zip.

Se trata de una aplicación en Java, así que tendréis que tener el JRE instalado previamente en vuestro equipo. No es necesario instalarlo, basta con que lo descomprimáis en el directorio que queráis y luego ejecutéis (desde Windows) el fichero lbe.bat

En la primera pantalla que os aparecerá al arrancarlo, "Connect", pulsad en "New" para definir un nuevo servidor. Empezaremos por la pestaña "Name", poned "Penn State University" en el único campo que aparece (por ejemplo). Pasamos a la pestaña "Connection", poned:

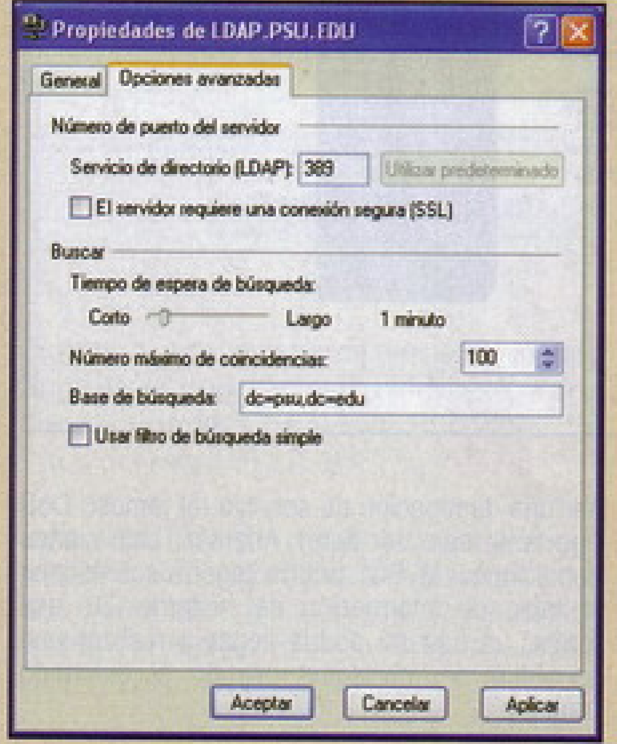
```
- Host: LDAP.PSU.EDU
- Base DN: dc=psu,dc=edu
```

Hecho esto podéis pulsar en "Save" y, de vuelta en la anterior pantalla, en "Connect". Ahora os aparecerá a la izquierda el listado de entradas (usuarios). Pulsando en uno cualquiera os aparecerán sus datos a la derecha.

Como podréis ver, os aparece mucha más información, como el departamento al que pertenece, su nombre de usuario, su shell en *nix, su grupo en *nix, su $home de usuario, etc. Mucha información que, en caso de ataque, puede venir muy bien.

La opción LDIF que os ofrece el programa os permite exportar las entradas a formato LDAP Data Interchange Format, un formato estándar que entienden los servidores LDAP a la hora de exporta e importar entradas.

Pero ahí no queda la cosa. Si editáis los datos de la conexión, en la pestaña "Connection" encontraréis el botón "Fetch DNs", que buscará qué otras raíces hay en el servidor LDAP. En el caso del ejemplo, al pulsarlo, veréis en "Base DN" que el desplegable nos muestra, entre otras opciones, CN=PWDPOLICY. Lo seleccionáis y os conectáis de nuevo al servidor.



Datos del servidor LDAP

Ahora, al seleccionar la raíz, os aparecerá información sobre la política de contraseñas, algo que podría ser muy útil a la hora de llevar a cabo un ataque con diccionario.

En fin, lo dicho, el LDAP puede resultar muy jugoso si se sabe jugar con él.

Si estáis intentando acceder a un servidor LDAP, y todavía no sabéis si permite el acceso sin utilizar contraseña (para invitados, como llevamos hecho hasta el momento), no hace falta que terminéis de crear la conexión, si después de introducir el nombre del servidor pulsáis en "Fetch DNs" y no aparece nada, lo más probable es que no os permita conectaros.

También podéis obtener información del servidor LDAP empleando el cliente LDAP que proporciona Microsoft entre sus utilidades de soporte técnico de Windows 2000, LDP. Por si tenéis difícil acceder a dicha aplicación, os lo dejamos en ldp.exe.

>>> Website del mes

"¡No soy el único! Siiiiiiii". Esto es lo que me salió del alma al conocer esta web: BugMeNot. Traducida podría significar "NoMeMolestes". ¿Estás harto de que para acceder un momento a un foro para leer un único post que te interesa tengas que registrarte? Inventarte tus datos, esperar a que te llegue un correo con una clave temporal, confirmar la clave y, después de más de 5 minutos, poder leer por fin el dichoso post para que al final ¡no sea lo que necesitabas!

Bueno, pues esta operación la realizamos todos los internautas decenas de veces al año, registrarte en webs que tienen la manía de obligarte a crear un usuario para controlar más los accesos.

Si estás harto de esta práctica abominable ¡visita BugMeNot!

En este website los usuarios suben logins y passwords de otras webs que te piden que te registres para acceder a la información alojada en ellas. No esperes encontrar un usuario y clave de una web de pago, dado que eso va contra las normas de la web (aunque alguna se pueda colar...), pero de entrada, el mero hecho de poder localizar un usuario ya creado y ahorrarte registrarte es todo un alivio. ¡Incluso hay plugins para ciertos navegadores de forma que el propio navegador consulta si hay algún login para esa web dichosa y lo introduce por ti!

Vamos, una maravilla. Así que si eres de los míos, visita **www.bugmenot.com.**



BugMeNot homepage

ATENCIÓN WEBMASTERS: Si creéis que vuestra web (bien sea independiente o de un grupo) es lo suficientemente buena como para aparecer en esta sección, y su contenido se refiere al hacking que aquí tratamos, no dudéis en hacérnoslo saber a la dirección cursodehack@megamultimedia.com.

Bugy Bugy

Este mes

El mes pasado vimos seguimos sacando las cosas más oscuras de algunas empresas famosas como Apple, que repetía aparición ese mes, Sun y Novell.

Este mes veremos otro poquito de todo y de todos porque ya sabéis que nos gusta darle a todos los palos para que nadie se queje luego de que tenemos preferencias por una u otra cosa. Por ello, este mes le vamos a dar a cosas muy variopintas que van desde MySQL a Apple pasando por el archiconocido Internet Explorer. Como siempre, si queréis saber más, tendréis que seguir leyendo porque hasta aquí os podemos contar.



Web de IBM

La información es poder

De siempre se ha dicho que la información es poder y esto hoy en día con toda la información que se mueve por internet es más cierto que nunca. Hoy la inmensa mayoría de servidores web que usamos van sobre Apache acompañado de un motor de bases de datos que igualmente suele ser en la mayoría de casos MySQL.

Y aquí precisamente está el cotarro que hace que una parte de la famosa pareja Apache-MySQL aparezca por aquí. Lo que os estaréis preguntando es qué parte será la culpable de dicho "desliz". Pues para no haceros esperar, os diremos que el culpable en esta ocasión es MySQL, ya que se ha detectado un par de bugs que lo traen hoy aquí. El primero es que las versiones anteriores a las 5.0.45 de la versión Community Server no requieren privilegios tales como "select" para la tabla origen para instrucciones del tipo "create table like" por lo que usuarios remotos podrían obtener información sensible que no debieran saber como la estructura de la tabla por ejemplo.

El otro bug afecta al motor InnoDB de MySQL que no realiza una correcta validación de los datos de entrada de tal forma que un usuario autenticado podría usar una sentencia "contains" creada especialmente para la ocasión para causar una denegación de servicio (el famoso DoS que tanto sale por aquí). Además, bajo ciertas condiciones, MySQL podría llegar a sobrescribir la tabla de información del sistema. De esa forma, un usuario podría llegar a realizar una escalada de privilegios usando el comando "rename".

Nuestro viejo amigo

Hacía ya algún tiempecillo que no salía por esta sección nuestro amigo Internet Explorer, el navegador más extendido de la red y no por ello el mejor. Claro que sobre gustos, como se suele decir, colores.



web de IE

El bug que trae en esta ocasión al navegador de Microsoft consiste en una explotación remota de una vulnerabilidad que permite a un atacante ejecutar código arbitrario en el contexto del usuario actual. El problema está localizado en el método setExpression de javascript que se implementó en mshtml.dll. Exactamente lo que ocurre es que es que, cuando se le pasan unos parámetros concretos (por supuesto con "mala idea"), la memoria puede corromperse de tal forma que Internet Explorer acceda a un objeto previamente borrado y de esa forma se estaría accediendo a todos los recursos a los que accedía dicho objeto.



web de Apple

Manzana, manzanita

Ya que estamos llegando al fin este mes, no nos vamos a olvidar del otro gran gigante actualmente tras Microsoft, nos referimos a Apple. Eso sí, no tiene que ver ni con los iPod, ni con los iPhone,... al menos de momento ;-)

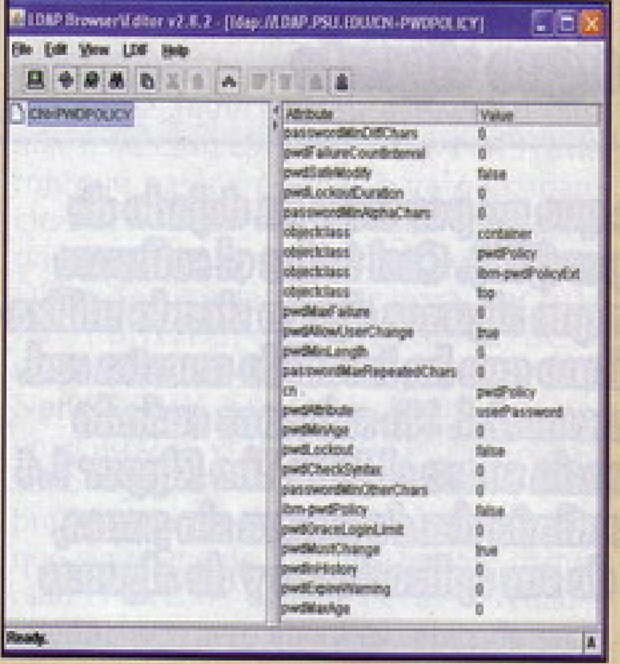
El problema descubierto consiste en una vulnerabilidad del tipo buffer overflow (desbordamiento de buffer) que puede llegar a permitir que un atacante ejecute código arbitrario con privilegios de root (administrador, superusuario, el que parte el bacalao por si alguien lo tiene más claro así). Dicho fallo está en la utilidad mount_smbfs y está confirmada la vulnerabilidad en el Mac OS X versión 10.4.10 tanto en la versión servidor como escritorio sin descartar además que las versiones anteriores pudieran estar afectadas.

Por último, el mensaje de siempre, si usáis algo de lo que sale aquí, actualizad, actualizad y mantened todo actualizado.



Búsqueda en el LDAP

Configurando el LBE



Política de contraseñas

Tampoco este programa necesita instalación, basta con ejecutar el ldp.exe, e ir a Connection ➠ Connect e introducir los datos del servidor LDAP.

Lo bueno de este programa, es que a la derecha veréis con pelos y señales la información que devuelve el servidor, así podréis conocer más sobre el servidor y sobre el protocolo.

En el ejemplo, podéis ver las versiones del protocolo LDAP que soporta el servidor, así como las opciones de cifrado de datos.

Si seleccionáis View ➠ Tree y a continuación introducís el "dc=psu,dc=edu", podréis ver a la izquierda la estructura de árbol del LDAP.

Si lo que queréis es descargar toda la información que pueda haber en un servidor LDAP, lo mejor será usar el LDAPminer dentro de LdapMiner-Win32-BIN.zip. Este programa también basta con copiarlo donde queráis usarlo. Eso sí, es posible que tengáis que poner el programa ldapminer.exe dentro de la librería libs (que incluye) para que no de problemas por falta de librerías.

Curiosidades de la vida, el LDAPminer fue creado por Sacha Faust, quien al poco tiempo de crear el programa entró a formar parte de la consultora PriceWaterhouseCoopers ¡si es que no hay "ná" como contratar a los que ya saben!

Esta aplicación permite recorrer todo el árbol del LDAP y sacar sus datos. Su uso es bien simple:

```
ldapminer -h [ servidor] -d
```

Así pues, para descargar todo lo que hay en el servidor donde estamos accediendo bastaría con ejecutar:

```
ldapminer -h LDAP.PSU.EDU -d
```

Además, el LDAPminer probará distintos fallos de configuración conocidos en los más populares servidores de LDAP si lo ejecutáis sin opciones:

```
ldapminer -h LDAP.PSU.EDU
```

Si no ejecuta ninguna prueba de seguridad, es porque el tipo de servidor LDAP no lo tiene entre los vulnerables.

Buscando un servidor LDAP con un portscanner

Otra posibilidad de encontrar servidores LDAP es buscando por el puerto TCP que utilizan, que es el 389. Para ello bastará con que utilicéis un escaneador de puertos como el SuperScan v4 al que le podéis indicar un rango de IPs probar y un puerto en concreto que localizar.

En la próxima entrega:
Borrando logs

Andrés Méndez Barco
Manuel Baleriola Moguel<



JOHN THE RIPPER

Un viejo rockero de la seguridad informática sigue vigente

Hoy pretendemos contaros las últimás virtudes de un viejo programa que no por viejo ha dejado de tener interés. Se trata de un antiguo programa llamado John The Ripper (JTR). Casi todos el software que nació en los años noventa han dejado de tener continuidad y aunque algunos siguen siendo utilizados, hace tiempo que dejaron de actualizarse, victimás del mercantilismo que ha invadido nuestra red. En este caso, John ha continuado a obtener soporte desde tiempo inmemorial. No sabemos cuándo nació pero el hecho es que en nuestro e-ezine hay una primera referencia sobre el John The Ripper 1.4 en el número 15 hacia 1998. Ha llovido bastante desde entonces y continúa dando guerra sin pausa, sin prisa pero sin detenerse. Vamos a hablar de la versión actual 1.7, de sus aplicaciones y de algunas de sus mayores contribuciones no oficiales.

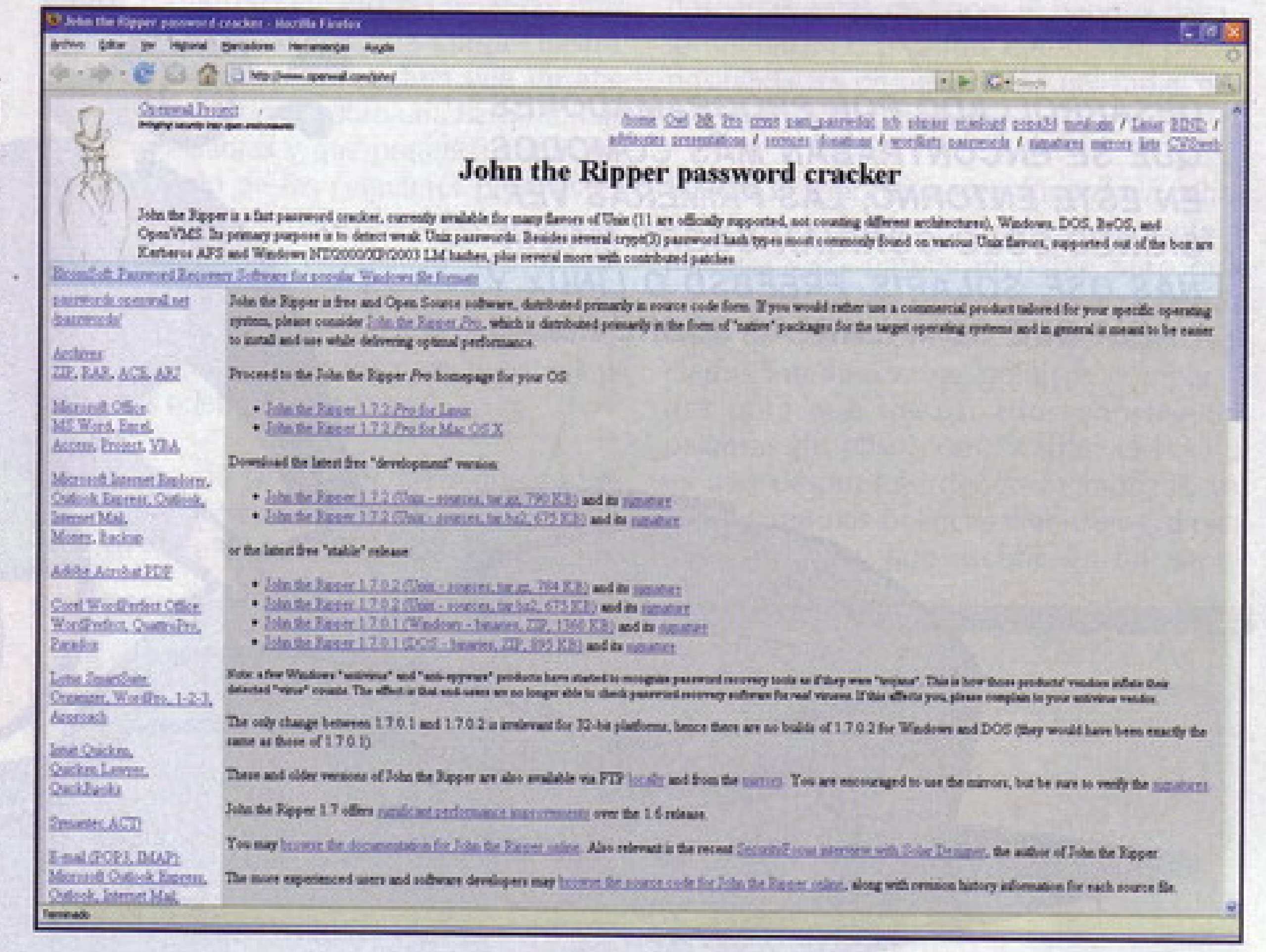


JTR. Un poco de historia

Este capitilo también se podría titular "Para despistados insignes", ya que todo el mundo que tuviera el interés en gastarse algunos euros en esta revista, debiera tener alguna idea y no ciertamente remota, sobre la historia de este soft, su utilidad y sus características principales, sin embargo, como para todo en esta vida, existen los recién llegados, os describiremos sucintamente cómo nació y para qué sirve.

En sus orígenes, JTR era un producto enfocado al cracking de las hash de un sistema UNIX. Desarrollado por programadores que se encontraban más cómodos en este entorno, las primeras versiones solo corrían sobre maquinas OSF, Solaris, FreeBSD o Linux y había que compilarlas sobre ellas. Sin embargo ya desde la versión 1.4 se podía obtener también ejecutables que funcionaban para DOS, Win95 y WinNT. Estas versiones habían sido compiladas con DJGPP v2, para la versión DOS y con la utilidad Cygnus Developer's Kit para la versión Win32. Desde sus orígenes se distribuyó bajo licencia "Open Source" en forma de código fuente que había que compilar localmente, sin embargo debido a la dificultad de encontrar compiladores gratuitos para la familia Windows, rápidamente se han ofrecido también ejecutables configurados para este sistema operativo.

La versión v1.4 que salio ahí por los años 97 fue la primera que ofreció soporte para las hash basadas en el algoritmo MD5. En la 1.5, un año más tarde se habían mejorado notablemente las rutinas para MD5, soportaba los formatos extended DES para BSDI, Blowfish para OpenBSD y mejorado las rutinas para atacar DES desde x86 con MMX sobre un Pentium II. El mismo año salio la versión v1.6 que por primera vez anunciaba su capacidad para atacar las hash LM de Windows NT. Tuvieron que pasar tres años para que apareciera la versión v1.6.3 donde se hacia el primer tentativo de vectorizar el ataque a DES y se ofrecía soporte para atacar Linux/PowerPC, FreeBSD/Alpha, SCO, OpenBSD/SPARC, OpenBSD/VAX, NetBSD/VAX, MacOS X, BeOS. Estamos en el 2007 y el "Openwall Project" ha sacado la versión v1.7.2 donde, como siempre, no han revolucionado el mundo sino que simplemente han tenazmente mantenido el nivel de calidad. Pocas novedades importantes, pero ahora es capaz de sacar provecho de las capacidades de los nuevos procesadores a 64-bit mode en modo extendido SSE2 y registros 16 XMM.



Sin embargo no es tanto de estas capacidades que queremos hablar como de las contribuciones no oficiales que el proyecto básico ha conseguido absorber y adaptar para un correcto funcionamiento. También nos gustaría dar un vistazo sobre en que se ha convertido el proyecto y dar algunas pistas de su extraordinaria longevidad en la red como proyecto abierto. De todas formás, sin o tenéis ganas de continuar y queréis conocer los datos directamente en la fuente, no tenéis más que pasaros por www.openwall.com/john/.

JTR. Situación actual

En realidad hoy Openwall es una empresa de servicios que dedica una parte de su tiempo a un subproducto llamado John The Ripper. Puede que sea esta la definición que a primera vista mejor se adapta al conjunto del proyecto, en realidad JTR es el gancho que probablemente atrae a posibles clientes para la empresa. Los artículos en venta se pueden clasificar en tres áreas. Los crakeadores específicos de diversos software, como archivos zip, rar, ficheros word y un largo etcétera, todos se venden como recuperadores de passwords olvidadas, pero también pueden tener otros usos, de todas formás, una experiencia personal en una empresa con la que tuvimos contacto, nos hizo ver que el negocio de la recuperación de passwords puede ser maá lucrativo de lo que parece. Un jefe de poca inteligencia es capaz de pagar sumás considerables de dinero con tal de recuperar un archivo importante, bloqueado con una palabra de paso que meses más tarde es incapaz de recordar. Verídico, aunque parezca imposible.

Otra área de negocio es la venta de diccionarios de palabras. Según cuentan su colección es el resultado de una búsqueda exhaustiva en la red de todos los diccionarios posibles en diversas lenguas. Esta puede que sea la característica principal de esta colección, ya que están representadas más de 20 lenguas diferentes, entre ellas el Afrikáans, Croata, Checo, Danes, Holandés, Ingles, Fines, Francés, Alemán, Húngaro, Italiano, Japones, Latín, Noruego, Polaco, Ruso,Español, Suahili, Sueco, Turco y Yidish. La razón de semejante colección no es solo dar soporte a diversas lenguas sino que un truco viejo como el mundo es poner una password en una lengua diferente al programa a proteger para despistar al posible atacante. El producto se vende bajo un CD que contiene un único archivo con más de 40 millones de entradas. Dicho producto puede obtener también directamente en la red en un ftp de uso restringido y accesible solo previo pago. EL que quiera probar suerte y atacarlo directamente, puede intentar ahorrarse los entre treinta y cin-

DESARROLLADO POR PROGRAMADORES QUE SE ENCONTRABAN MÁS CÓMODOS EN ESTE ENTORNO, LAS PRIMERAS VERSIONES SOLO CORRÍAN SOBRE MAQUINAS OSF, SOLARIS, FREEBSD O LINUX Y HABÍA QUE COMPILARLAS SOBRE ELLAS



cuenta dolares que cuesta la colección. No sabemos su eficacia, de la colección, ya que nunca lo hemos probado, pero siempre abra gente disponible a comprar cosas del estilo.

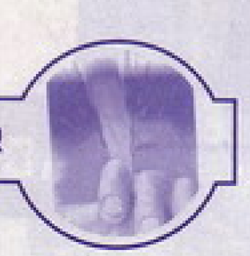
En tercer lugar, openwall se financia mediante la venta de una distribución especifica linux, dedicada específicamente para servidores de red muy expuestos a ataques. Se denomina Openwall GNU/*/Linux (OWL) y es compatible con la mayor parte de las distribuciones comerciales de linux. No sabemos porque, pero hay una oferta especial para Rusia. Si os pasáis por este país o tenéis un amigo de esta nacionalidad, podéis obtener un descuento. Como hemos dicho antes, es una distribución enfocada a la seguridad y prevista para ser utilizada como servidor de red.

Por ultimo, Openwall, ofrece servicios diversos de asesoría de seguridad. Tenemos la impresión que nada de todo esto hace nadar en la abundancia a su creador, pero por un lado llena el plato de su mesa todos los días y ha mantenido la popularidad de JTR, lo que explica su larga permanencia en la red, así como las diversa variantes que han surgido y que sin tener soporte oficial, si que han recibido publicidad en su web. De todas ellas las que más nos han interesado y hablaremos en este articulo son la versión JUMBO con el soporte para "mscash" y la versión para computación distribuida.

JTR Jumbo Pach

Antes que nada hablaremos de todas las mejoras que sin esta soportadas por los creadores de John, reciben publicidad gratuita y se pueden obtener directamente desde su web. Todas ellas se encuentran disponibles bajo forma de código fuente y distribuidos en forma de ficheros diff. Hay bastantes cosas interesantes para el que se encuentre frente a un problema especifico y quiera hacer un ataque especifico sobre un tipo de cifrado inusual y bajo un sistema operativo exótico. ¿Estáis interesados sobre un ataque a Netscape LDAP SHA, SSHA ? Pues ahí tenéis la solución. Alguien,... no, alguien in concreto no, un tal K Evangelios y otro que se hace llamar Sun-Zero, se han quemado las pestañas y los dedos sobre un teclado para encontraros la solución. Como este ejemplo hay unos cuantos. Alain Espinosa ha creado un patch que ataca las credenciales guardadas por Windows para poder arrancar una maquina que se encuentra desconectada del "dominio" que debe darle acceso. Hemos hablado de ello en otros artículos así como la utilidad creada por Arnaud Pilon, llamada CacheDump, que extrae de una maquina la hash correspondiente. Esta utilidad hace las delicias de muchos atacantes de redes privadas cuando hay acceso físico a las maquinas y abre después grandes horizontes para ulteriores ataques. Dada la gravedad de la vulnerabilidad, casi todos los antivirus comerciales que se precien, detectan esta utilidad y la ponen en cuarentena, ello implica que debe desconectarse en antivirus antes de lanzarlo, lo cual tampoco es tan sencillo de hacer en los modernos ambientes empresariales.

Volviendo a esta utilidad, es tal su peligrosidad que empieza a ser difícil de encontrar en los sitios habituales donde antes se localizaba en http://www.cr0.net:8040/misc/cachedump-1.2.zip pero hay todo intento de encontrarla ahí da como resultado un sitio inaccesible. Es todavía posible encontrarla en la web de Openwall o bien en sitios como http://www.mirrors.wiretapped.net/security/host-security/john/contrib/cachedump/. De todo ello se desprende que Microsoft ha empezado la caza y captura. El que tenga una copia de esta utilidad, más vale que se la guarde cifrada, ya que es posible



que en breve plazo incluso la versión zipeada sea localizada por los antivirus y puesta en cuarentena.

Volviendo a nuestro pach monstruoso, para ahorrarnos el trabajo de buscar la que nos convenga, Erik Winkler ha hecho un esfuerzo unificador y ha publicado un patch "madre y padre" de todos los patchs. A partir de ahí todo ser viviente debería ser capaz de compilar y linkar obteniendo un ejecutable. Fácil. En teoría. En la practica es bastante fácil hacerlo sobre un OS nativo si esta previsto en el script Makefile. En la practica es un poco más difícil si la distribución linux que utilizamos es un poco especial. Si lo que deseamos por algún motivo es hacerlo sobre un Vmware, puede que tengamos problemás. De hecho si por ejemplo queremos compilar bajo cygwin, no hay forma de hacerlo si antes no hemos instalado libdes, que de todas formás podemos encontrar en http://www2.psy.uq.edu.au/~ftp/Crypto/DES/.

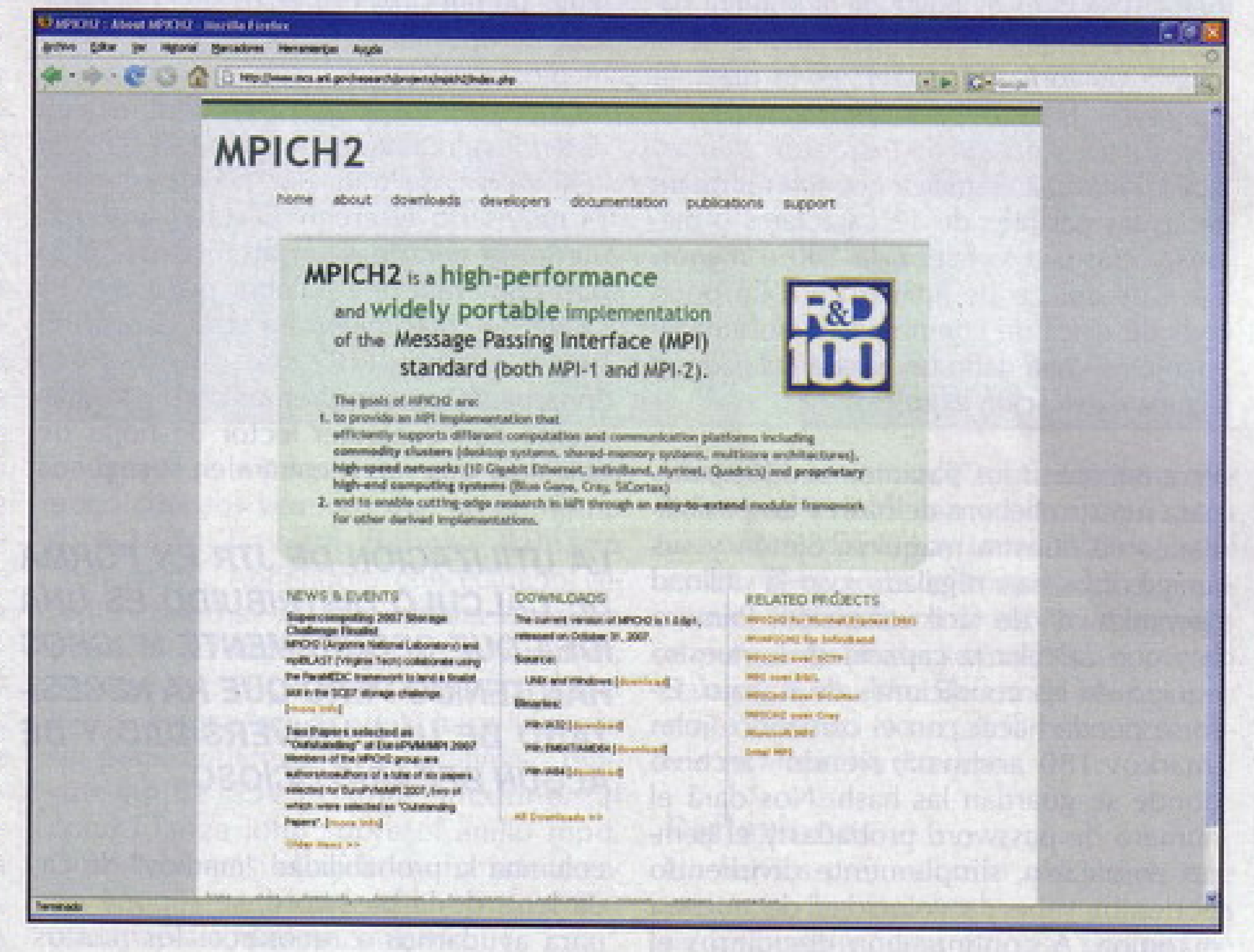
Para librar de estas amarguras a los amantes de Windows, Thomás Springer se ha tomado la molestia de compilarlo y se encuentra disponible en la web de Openwall. El ejecutable soporta diversos formatos que la versión principal desdeña por diversas razones. Puede que no deseen de manera oficial provocar la iras de Microsoft. El caso es que MS-Cache-Hash , NTLM, Kerberos, NSLDAP, Eggdrop, Dominosec, Lotus v5 Proprietary, Invision Power Board 2.x salted MD5, Apache MD5, Post.Office MD5, MySQL, Raw MD5, Raw SHA1, todos ellos están presentes y listas para ser atacados dentro de u na sesión "cmd" de win32.

Sin embargo hay otras posibilidades que solo si se busca en el ftp de openwall o si se esta dado de alta en su lista de distribución podemos conocer. Estamos hablando de la opción basado en las reglas Markov o de la posibilidad de utilizar la plena potencia de un equipo dual core.

JTR versión Markov

Esta versión se basa sobre los trabajos de un matemático ruso llamado Andrei Markov. Este buen hombre demostró la probabilidad de una serie de eventos encadenados. Probablemente vamos a recibir una montaña de mensajes quejándose de esta escuálida definición pero es la forma más rápida de explicar el descubrimiento estadístico de este matemático. Esta propiedad estadística se aplica para seleccionar de un diccionario las palabras más probables para atacar una cierta "hash". Imaginamos que todos saben que un ataque de fuerza bruta sobre una hash de más de ocho palabras y que pretenda cubrir todo el espacio de los caracteres posibles es totalmente inabordable para las maquinas actuales. La única posibilidad son los ataques mediante diccionarios o mediante diferentes simplificaciones del tipo de trasponer caracteres, añadir ciertos caracteres, eliminar otros o intercalar terceros.

En el caso de las aplicaciones que se basan en los descubrimientos de Markov, lo que se hace es utilizar un diccionario, pero solo utilizar las palabras que por alguna razón suponemos que tienen más probabilidades de ser utilizados por el humano que la inventó. Uno de las estrategias posibles es seleccionar un conjunto de palabras de paso, calcular la probabilidad de aparición del primer carácter de cada palabra, después calcular la probabilidad de que aparezca un cierto carácter a continuación. Es posible asociar de esta forma a cada palabra del diccionario y descartar antes de hacer el penoso calculo del hash las palabras que tienen pocas posibilidades de haber sido utilizadas por una persona (humana).



EN REALIDAD HOY OPENWALL ES UNA EMPRESA DE SERVICIOS QUE DEDICA UNA PARTE DE SU TIEMPO A UN SUBPRODUCTO LLAMADO JOHN THE RIPPER

Este es el soporto matemático de la estrategia, pero detrás se esconde algo que a primera vista parece increíble pero que en la realidad es absolutamente cierto. Es inútil que las empresas y los softwars asociados intenten crear políticas complicadas para que los usuarios construyan palabras de paso complicadas, el hecho es que después se deben memorizar, ya que las mismás políticas y consejos, dicen que jamás hay que escribir en un papel una password importante. Si un humano tiene que recordar algo, de una forma automática intentara asociar la secuencia de caracteres a algo que le permita reproducir la secuencia que en su día tecleó sobre el terminal. Parece cosa de magia pero lo cierto es que en no importa que idioma, la secuencia de caracteres tiende a seguir un mismo patrón. Las limitaciones de la memoria humana hacen que la entropía de las palabras de paso creadas por un humano sea realmente pequeña, inferior a 32 bits según un estudio del NIST de 2004. Esta técnica se utiliza también en los sistemás de reconocimiento de palabras en los ordenadores que siguen ordenes habladas o en los modernos equipos de mecanografía hablada.

Sea la razón y el substrato matemático el caso es que la reducción de las búsqueda de una palabra de paso ha sido introducida en el patch de JTR diseñado por Simon Marechal <simon@banquise.net> y presenta unas características muy interesantes así como su utilización y parametrización. La versión que hemos probado es la que corre bajo window y ha sido compilada con cygwin por el mismo equipo de Marechal. Para los conocedores de JTR solo presenta una única opción extra que se parametriza con la sintaxis siguiente "-markov:LEVEL: START:END:LENGTH" donde "LEVEL" es un valor sin dimensiones que da una idea de la "fortaleza" máxima de las hash a romper, "START" es el indice de la primera palabra a chequear, "END" es el indice de la ultima palabra, "LENGTH" es la máxima longitud a probar. En el ejemplo dado por los autores en su distribución "--markov:100:0:0:12" significa que john probara todas las palabras de 12 caracteres o menos y con una fortaleza de 100 o menos. Fácil de aplicar de aplicar pero un poco más de difícil de comprender. Afortunadamente nos han dado un par de utilidades y alguna explicación extra.

Para encontrar los parámetros adecuados para nuestro fichero de hash y las posibilidades de nuestra maquina, Simón y sus amigos nos han regalado con la utilidad "genmkpwd" de fácil utilización. Primero hay que calcular la capacidad de nuestro equipo en las condiciones de trabajo. Esto se puede hacer con el comando "john -markov:180 archivo", siendo "archivo donde se guardan las hash. Nos dará el numero de password probadas y el tiempo empleado, simplemente dividiendo podemos saber la velocidad de nuestra maquina. A continuación decidimos el tiempo que deseamos emplear en la tarea y, esta vez multiplicando calculamos el numero de candidatos a probar. Es el momento de utilizar el programa "genmkvpwd" cedido por los autores. Con un simple "genmkvpwd stats 0 12" veremos pasar por nuestro terminal un dato (lvl) seguido por el numero de password a probar. Basta con memorizar el valor "lvl" que se ajusta al numero de password que queremos probar. Este es el valor a utilizar como "LEVEL"

De todas formás no hay que olvidar que el algoritmo de markov funciona en base a un estudio estadístico. La pregunta es de donde sale este análisis. Si viene dado por alguien externo que resida en las llanuras de Texas, por ejemplo, las estadísticas representaran el modo de hablar, comportarse y expresarse de los tejanos. Si queremos atacar una palabra de paso escrita por un ucraniano, de poco nos va a servir. Nos hace falta un texto, un diccionario, algo desde el cual podamos extraer las pautas. La solución nos la da el mismo autor con la utilidad "calc_stat". Basta teclear rellenar o encontrar un archivo con las palabras que penséis sean más representativas del lenguaje, llamarlo por ejemplo "archivo" y teclear "calc_stat archivo stats". Generareis un archivo llamado "stats" con las estadísticas necesarias.

Finalmente si queremos hacer un "tunning" de nuestros esfuerzos o ver la fortaleza de nuestras estadísticas en un cierto medio, o a la inversa, saber que fortaleza teórica tiene nuestra password frente a un determinado ataque, también nos ofrecen la solución. Se trata de "mkvcalcproba". Es necesario el archivo "stats" anteriormente generado y un archivo de texto que contenga una palabra por linea. La salida de "mkvcalcproba stats passwordlist > prueba.txt" sera un fichero "prueba.txt" que podremos abrir cómodamente con cualquier lector de hojas de calculo y que nos mostrara en la segunda columna la probabilidad "markov" de cada letra de la password, se supone que para ayudarnos a reconocer los puntos débiles, en la tercera columna la "fortaleza" markov y en la quinta la clasificación de ser adivinada por un ataque de fuerza bruta clásico, es decir, estúpido.

LA UTILIZACIÓN DE JTR EN FORMA DE CÁLCULO DISTRIBUIDO ES UNA IDEA QUE SEGURAMENTE MUCHOS HAN TENIDO PERO QUE HA NECESITADO DE UNA UNIVERSIDAD Y DE ALGÚN BECARIO OCIOSO

De todas formás, en cualquier caso hace falta potencia de maquina para poder conseguir encontrar la palabra de paso de nuestros suenos y todas las variaciones de JTR que hasta ahora hemos comentado, adolecen de un defecto. No son capaces de trabajar en forma de trabajo distribuido y no utilizan la potencia total de los modernos "dual core".

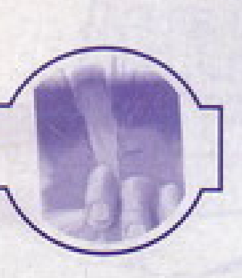
Por alguna razón solo por ellos conocida, "Alexander Peslyak" creador e impulsor del proyecto se niega a distribuir de forma oficial una distribución que funcione de forma automática sobre un procesador dual. Simplemente da consejos de como manualmente se puede configurar un ataque sobre diversos procesadores a base de jugar con el modo "incremental" y diversas configuraciones "MinLen" y MaxLen". Sin embargo si que da acogida, aunque sin publicidad de diversos intentos para crear variantes de JTR que pueden realizar ataques sincronizados desde diversas maquinas o bien utilizar toda la fuerza de un "dual core". Hablemos de esto.

JTR versión dual

La utilización de JTR en forma de cálculo distribuido es una idea que seguramente muchos han tenido pero que ha necesitado de una Universidad y de seguramente de algún becario ocioso para que el proyecto viera la luz. El primer informe sobre el proyecto data de mediados de 2004, aunque después han continuado sacando versiones a medida que JTR publicaba una versión estable. Nos estamos refiriendo al trabajo realizado por Ryan Lim en la Universidad de Nebraska-Lincoln.

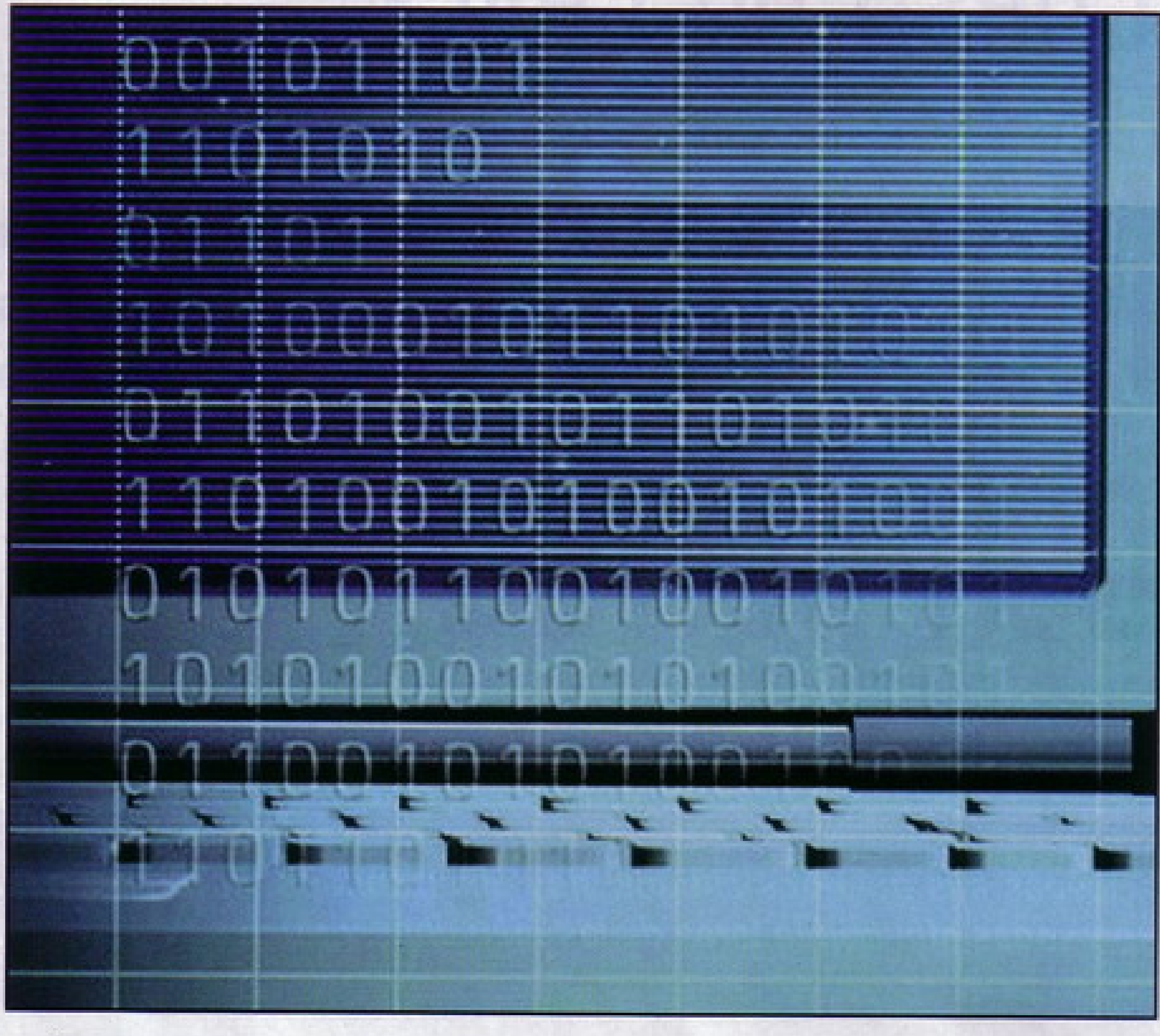
Cuando nos descargamos y descomprimimos john-1.7.2-bp17-mpi.gz lo primera que hay que hacer es leerse el README y ahí nos dicen que para compilar los fuentes hace falta que se encuentre instalado previamente algo parecido a MPI. Estas siglas corresponden a "Message Passing Interface" y se refiere a un conjunto de utilidades bastante utilizadas en medios universitarios para crear trabajos distribuidos entre varios ordenadores. Para hacer las pruebas nosotros hemos utilizado la versión MPICH2 que podéis encontrar en http://www.mcs.anl.gov/research/projects/mpich2/index.php.

Existe la versión para Win y la versión para Unix, pero la primera requiere Microsoft Developer Studio y Microsoft SDK, demásiadas cosas que requieren registro para nuestro gusto, así que nos decidimos a hacer las pruebas en una maquina que alojaba un humilde UBUNTU. No se requiere nada más que un compilador C++ y un Python 2.2, todo ello o bien se encuentra ya en la distribución o bien con un apt-get es fácilmente instalable. Después la instalación de MPICH2 es un poco más laboriosa, pero si se siguen las instrucciones atentamente no hay grandes dificultades y se acaba con un sistema capaz de crear anillos de comunicación protegidos con una palabra de paso, con lo cual, en teoría, pode-



mos incluso crear una red distribuida sobre una red publica, aunque no parece que la seguridad sea extrema ya que no fue la máxima prioridad de sus creadores. Para lanzar los trabajos la utilidad que necesitamos se llama mpiexec y se utiliza en la forma "mpiexec -n x ejecutable", siendo "n" el numero de nodos.

Una vez instalado MPICH2, es necesario probar que podemos crear un anillo aunque sea dentro de nuestra maquina. No es difícil pero requiere leerse las instrucciones más de una vez para aprender a configurar correctamente las comunicaciones y también es aconsejable el apartado que se refiere a la seguridad, porque sino podemos crear un agujero de seguridad enorme en nuestra maquina. No olvidemos que estamos creando algo que esta diseñado para poder lanzar ejecutables a distancia. Fue un trabajo de varios días.



Cuando pensamos que lo peor había pasado, descomprimimos e intentamos compilar la versión MPI de John, nos encontramos con varias dificultades más. La primera es que las instrucciones que encontramos en el README no funcionan en absoluto. Es una de las pocas veces en que se gana tiempo si uno pasa de leerse la ayuda y desgraciadamente no fue nuestro caso. Resulta que hacer "make.sh clean" y " make.sh" solo sirve para encontrarse con mensajes de error. Afortunadamente el clásico "make clean linux-x86-sse2" funciona,... hasta cierto punto. Seguimos encontrando problemás de compilación y el script no conseguía encontrar algo llamado "lcrypto", aparentemente una librería que pertenece a alguna de las utilidades de openssl. UBUNTU tiene la utilidad de instalación de paquetes llamada "synaptic". Un poco a la desesperada y después de instalar openssl-dev sin éxito, buscamos todas los paquetes con referencias lcrypto y encontramos tres. "Libcurl3-dev", "Libcurel3-openssl-dev" y "Libwww-curl-perl". No nos complicamos la vida, instalamos las tres y se acabó el problema.

Como en la versión standard, el ejecutable se encuentra en el directorio "run" con el nombre de "john" y funciona aparentemente como la versión normal, lo que pasa es que si se utiliza como estamos acostumbrados estamos en las mismás condiciones que al principio del articulo, o sea un "john" que funciona sobre un solo procesadores e ignora al resto. No hay en ningún sitio instrucciones ni nada que se le parezca, pero si somos un poco curiosos veremos que en el mismo directorio hay un fichero llamado "run_all.sh". Abriéndolo con cuidado veremos que hay cuatro instrucciones. La primera "#!/bin/sh" abre un terminal sh, la segunda "PROCS=$1" crea una variable, la tercera "rm -f core.*" hace limpieza sin pedir confirmación y la ultima " mpirun -np $PROCS ./john -incremental crack" lanza john sobre el anillo mpd. Dos problemás; el anillo no ha sido creado; hay que cambiar la ultima instrucción y adaptarla a nuestro contorno.

Para crear el anillo hay que abrir otro terminal (estamos bajo linux), leerse las instrucción MIPCH2 donde dicen que hay que crear un fichero llamado mpd.conf en el directorio "/etc/" con una unica linea "secretword=<palabra que os de la gana>", y darle derechos de lectura y escritura solo a root mediante la instrucción "chmod 600 mpd.conf". Después hay que lanzar el anillo con la instrucción "mpd". Si no se cumplen ambas condiciones el anillo se niega a arrancar advirtiéndonos claramente del motivo, en este caso no hay mensaje esotéricos. La modificación de la instrucción consta en cambiar el ejecutable "mpirun" por "mpiexec" ya que estamos empleando una versión más moderna de mpi, substituir "-np" por "-n 2" y evidentemente "crack" por el fichero que contiene las hash en vuestro caso. Una vez arrancado no hay forma fácil de ver el estado de avance de la operación y si paramos john de la forma habitual corremos el peligro de perder todo el trabajo. Es un trabajo distribuido. Debemos utilizar otro script llamado clean_all.sh que encontrareis en el mismo directorio.

Reflexiones

No hemos profundizado mucho en este proyecto, hay mucho que estudiar. Una de las posibles ideas es crear una red de maquinas normales que empleen esta técnica para participar en un proyecto común. Los trabajos que son bien conocidos en el mundo del tipo SETI@home han sido configurados sobre un principio totalmente distinto, pero para hacerlo primero hay que estudiar la inplantación de "mpich2" de forma transparente y fácil sobre un Windows standard de los que corren a millones en el mundo. Queda este trabajo para otros, en todo caso esperamos que si alguno se plantea el reto se divierta tanto como nosotros haciendo estos pequeños, e incompletos, ensayos.

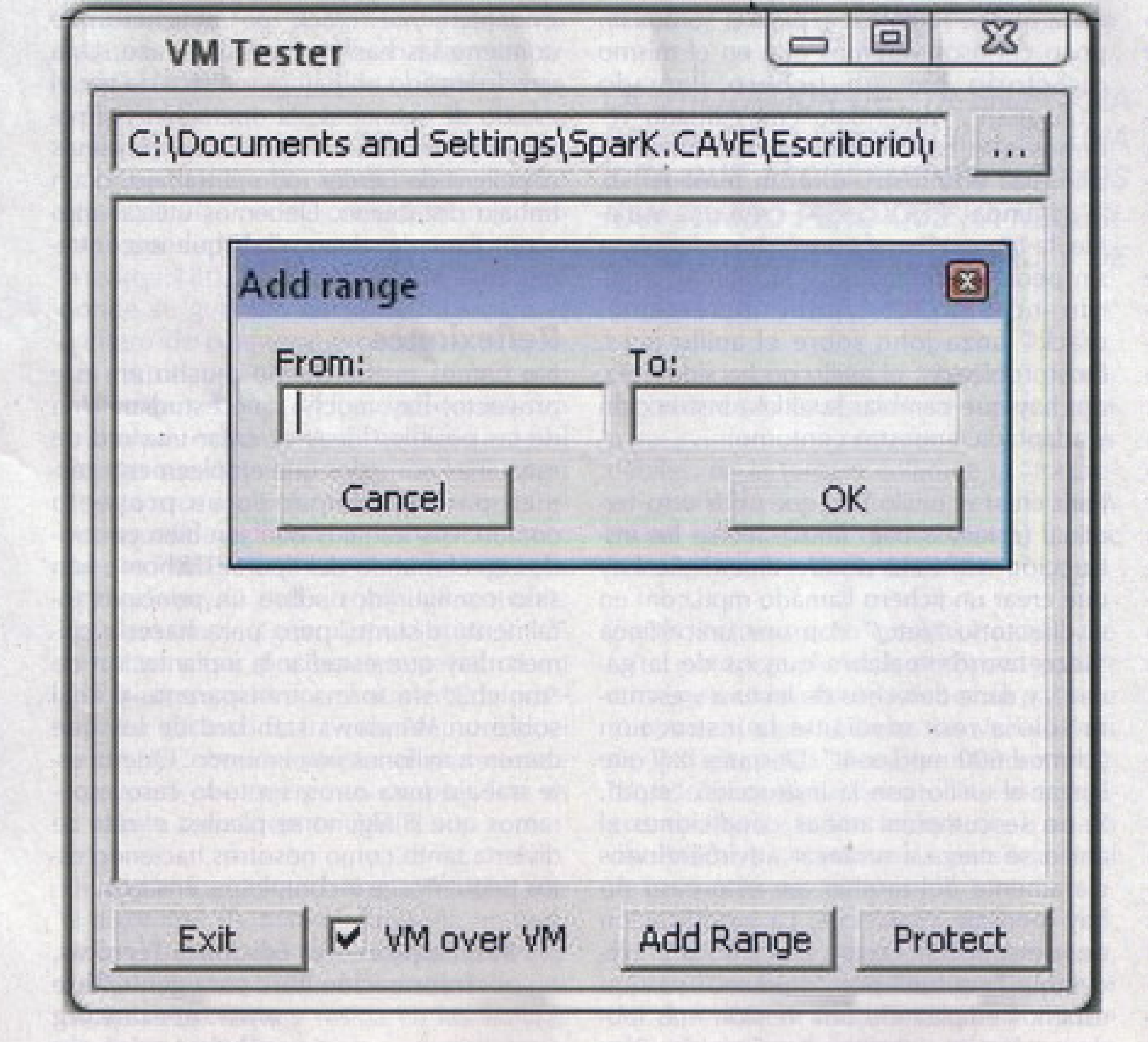
SET, Saqueadores Ediciones Técnicas.
Información libre para gente libre
www.set-ezine.org
web@set-ezine.org

CURSO de CRACK

Máquinas Virtuales con REWOLF

Proyectos GNU

Buenas mis queridos amigos, hoy analizaremos un proyecto que ya circula por la red juntando personas afin con la tarea de las máquinas virtuales (VM), incluyéndome yo.



Protectorrewolf

Por si no lo recuerdan

Ya he explicado en números anteriores de que se tratan las VM, hoy en día numerosas protecciones cuentan con esta característica, pero describiré en pocas palabras de que se trata.

Las protecciones por VM, instalan una máquina virtual en el ejecutable, y convierten partes vitales del programa a proteger en código propio de la VM, para ser interpretado por esta.

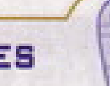
Esta estrategia complica el análisis de la víctima, ya que los códigos de operación son distintos que los de la arquitectura x86. Pueden ser dinámicos, aleatorios, nuevos por cada VM, e inclusive pueden mutar, junto con la VM.

Utilizando también métodos criptográficos y o de ofuscación, además de contener algoritmos de chequeo de integridad.

Es una buena técnica contra el análisis por parte de personas no expertas en la materia, es decir, anti-novatos :).

Lo que veremos hoy

Como mencioné antes, estudiaremos un poco el proyecto de un cracker conocido llamado rewolf. Se trata de un "virtualiza-



>>> Listado 1

```
\bin\loader\meta.exe                      - cargador o loader compilado
\bin\protector\x86.virt.exe               - el virtualizador compilado
\bin\test_app\vm_test.exe                 - aplicación de ejemplo compilada
\bin\test_app\vm_test_vmed_01.exe         - aplicación ejemplo con una capa de VM
\bin\test_app\vm_test_vmed_02.exe         - aplicación ejemplo con dos capa de VM
\doc\x86.virt.after.gif                   - diagram - represents executable after virtualization
\doc\x86.virt.before.gif                  - diagram - represents executable before virtualization
\doc\x86.virt.pdf                         - documentación
\src\loader\loader.asm                    - código fuente del cargador
\src\protector\common.cpp                 - algunas funciones comunes
\src\protector\common.h                   - archivo cabecera para las funciones comunes
\src\protector\hde.h                      - archivo cabecera para Hacker Disassembler Engine
\src\protector\hde.lib                    - archivo librería para Hacker Disassembler Engine
\src\protector\macros.h                   - archivo cabecera para macros auxiliares
\src\protector\main.cpp                   - programa principal (gui, manejo de PE, etc...)
\src\protector\poly_encdec.h              - versión binaria de algoritmos polimórficos_(enc/dec)
\src\protector\protect.cpp                - parte principal de la engine de virtualización
\src\protector\protect.h                  - archivo de cabecera para la engine de virtualización
\src\protector\res.rc                     - archivo de recursos
\src\protector\resource.h                 - archivo de cabecera para los recursos
\src\test_app\main.cpp                    - código fuente de la aplicación de ejemplo
\src\test_app\res.rc                      - archivo de recursos de la aplicación de ejemplo
\src\test_app\resource.h                  - archivo cabecera para la aplicación ejemplo
```

>>> Listado 2

```
void doProtect(HWND listBox, bool vmovervm, char* fileName)
{
      HANDLE hFile = CreateFile(fileName, GENERIC_READ, FILE_SHARE_READ, 0, OPEN_EXISTING,
FILE_ATTRIBUTE_NORMAL, 0);
      if (hFile == INVALID_HANDLE_VALUE) ERROR("Cannot open input file.");
      DWORD tmp;
      DWORD fSize = GetFileSize(hFile, 0);
      BYTE* hInMem = (BYTE*)GlobalAlloc(GMEM_FIXED, fSize);
      if (!hInMem) ERROR("Cannot allocate memory.");
      ReadFile(hFile, hInMem, fSize, &tmp, 0);
      CloseHandle(hFile);

      IMAGE_NT_HEADERS* inh = (IMAGE_NT_HEADERS*)(hInMem + ((IMAGE_DOS_HEADER*)hInMem)-
>e_lfanew);
      IMAGE_SECTION_HEADER*    ish    =    (IMAGE_SECTION_HEADER*)(hInMem    +
((IMAGE_DOS_HEADER*)hInMem)->e_lfanew + inh->FileHeader.SizeOfOptionalHeader + sizeof(IMA-
GE_FILE_HEADER) + 4);
```

dor", es decir, un programa que genera una máquina virtual, o posee una máquina virtual, toma la zona de código que se le indique, adaptando su lógica y utilizando los operandos de la máquina virtual.

En definitiva, convierte el código ensamblador a código interpretado por la máquina virtual.

Explicaré y veremos el código fuente de este invento, obviamente, no funciona siempre y tiene errores, pero eso no nos incumbe aún. :)

Veremos primero que contiene el paquete, ni bien lo bajamos de la página de rewolf: (ver Listado 1)

Empezando por el principio

Bien, señores, tomaremos el toro por las astas, podemos probar las dos aplicaciones de ejemplo que trae el paquete y veremos que la que posee dos capas de VM (es decir, una VM dentro de otra, donde la segunda es código interpretado que interpreta la primera, pero a su vez, la segunda VM posee código interpretado, que es parte del programa) es mucho más lenta que la primera, tanto al hacer cálculos de MD5, como al dibujar.

Empezaremos a mirar el fichero main.cpp, analizando las partes más importantes de la función doProtect. (ver Listado 2)

Como estamos analizando aquí arriba, la función comienza abriendo el fichero, controlando esta apertura por errores, y luego definiendo las constantes del ejecutable, la cabecera, y los datos de las secciones en la cabecera. (ver Listado 3)

>>> Listado 3

```
        //chequeos por relocs
        DWORD rel = 0;
        if  (inh->OptionalHeader.DataDirectory[IMAGE_DIRECTORY_ENTRY_BASERELOC].VirtualAd-
dress)
        {
                rel  =  rva2raw(inh->FileHeader.NumberOfSections,  ish,  inh->OptionalHeader.Da-
taDirectory[IMAGE_DIRECTORY_ENTRY_BASERELOC].VirtualAddress);
                if (rel == 0xFFFFFFFF) ERROR("Invalid relocations RVA.");
                rel += (DWORD)hInMem;
        }
```

>>> Listado 4

```
        int itemsCnt = SendMessage(listBox, LB_GETCOUNT, 0, 0);
        if (!itemsCnt) ERROR("Nothing to protect (add at least one range).");
        DWORD* items = (DWORD*)GlobalAlloc(GMEM_FIXED, itemsCnt*8);
        DWORD* items2 = (DWORD*)GlobalAlloc(GMEM_FIXED, itemsCnt*8);
```

x86.virt.before

>>> Listado 5

```
        BYTE* hVMMemory;
        DWORD vmInit;
        DWORD vmStart;
        srand(time(0));
        int vmSize = vm_init(&hVMMemory, &vmInit, &vmStart);
```

Aquí arriba, se lleva a cabo el chequeo por la sección de relocations, si existe. Esta sección sirve para "ayudar" al cargador de windows, a alinear el ejecutable, o brindar alguna dirección e información sobre algo que no pueda resolver.

Si el loader de windows puede resolver todo cuando carga ese archivo, entonces la sección relocations será obviada. (ver Listado 4)

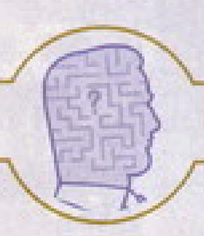
Si vemos la aplicación principal, veremos que podemos elegir como dije, una sección de código, es decir, una zona, y esto es almacenado en un listbox, que luego utiliza para ir obteniendo las zonas elegidas, y las va protegiendo. (ver Listado 5)

ESTA ESTRATEGIA COMPLICA EL ANÁLISIS DE LA VÍCTIMA, YA QUE LOS CÓDIGOS DE OPERACIÓN SON DISTINTOS QUE LOS DE LA ARQUITECTURA X86

Podemos entender aquí arriba las 3 variables principales para inicializar la Virtual Machine. Luego se crea un número aleatorio y finalmente se inicializa la VM, donde se pasa el puntero donde residirá la VM.

Luego se pasa también la dirección de inicio y de comienzo, como verán no se trata de lo mismo. :)

Ahora veamos que sucede dentro de la función vm_init: (ver Listado 6)



>>> Listado 6

```
int vm_init(BYTE** retMem, DWORD* _vmInit, DWORD* _vmS-
tart)
{
        HANDLE hVMFile = CreateFile("loader.exe",
GENERIC_READ, FILE_SHARE_READ, 0, OPEN_EXISTING, FILE_AT-
TRIBUTE_NORMAL, 0);
        DWORD vmFileSize = GetFileSize(hVMFile, 0) - 0x400;
        if (hVMMemory) GlobalFree(hVMMemory);
        hVMMemory = (BYTE*)GlobalAlloc(GMEM_FIXED, vmFileSi-
ze);
        SetFilePointer(hVMFile, 0x400, 0, FILE_BEGIN);
        DWORD tmp;
        ReadFile(hVMFile, hVMMemory, vmFileSize, &tmp, 0);
        CloseHandle(hVMFile);
```

>>> Listado 7

```
        __vmSize = *(DWORD*)hVMMemory;
        DWORD vmSize = *(DWORD*)hVMMemory;
        DWORD vmCodeStart = *(DWORD*)(hVMMemory + 4);
        DWORD _ssss = (*(DWORD*)(hVMMemory + 28))*4 +
(*(DWORD*)(hVMMemory + 32))*8 + 4;
        *_vmInit = *(DWORD*)(hVMMemory + 8) - _ssss;
        *_vmStart = *(DWORD*)(hVMMemory + 12) - _ssss;
        DWORD vmPoly = *(DWORD*)(hVMMemory + 16);
        DWORD vmPrefix = *(DWORD*)(hVMMemory + 20);
        DWORD vmOpcodeTab = *(DWORD*)(hVMMemory + 24);
        *retMem = hVMMemory + _ssss;
```

permutaterewolf

Bien, lo primero que se hace en la función vm_init, es abrir el loader o cargador, y obtener el tamaño de la VM.

Luego reserva una cantidad de memoria, según el tamaño obtenido, a partir del puntero pasado en la variable hVMFile.

>>> Listado 8

```
//XOR val 0x34 val
//SUB val 0x2C val
//ADD val 0x04 val
//XOR CL  0x32 0xC1
//SUB CL  0x2A 0xC1
//ADD CL  0x02 0xC1
//INC     0xFE 0xC0
//DEC     0xFE 0xC8
//ROR CL  0xD2 0xC8
//ROL CL  0xD2 0xC0
//junk    0xEB 0x01 xx
```

Finalmente lee del fichero y cargando toda la VM en la memoria reservada. (ver Listado 7)

En éstas líneas de aquí arriba se toman los parámetros básicos de la VM, como por ejemplo, las direcciones de comienzo, tamaño, dirección de la función polimórfica de encripción y desencripción, además del listado de códigos de operación (OpcodeTab).

```
GenPolyEncDec();
```

Esta función de aquí arriba, genera decriptores y encriptores polimórficos, es decir, son diferentes por aplicación protegida.

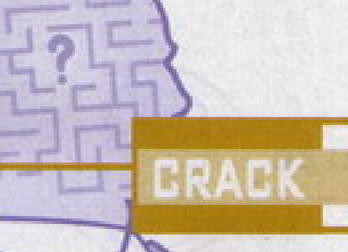
SE TRATA DE UN "VIRTUALIZADOR", ES DECIR, UN PROGRAMA QUE GENERA UNA MÁQUINA VIRTUAL, O POSEE UNA MÁQUINA VIRTUAL, TOMA LA ZONA DE CÓDIGO QUE SE LE INDIQUE

Como veremos en los fuentes, el autor, muestra el original comentado, luego se hace el proceso. (ver Listado 8)

Veremos que se trata de una rutina de cifrado bastante simple y rapida por cierto, utilizada en diferentes virus, con mayor o menos modificaciones. (ver Listado 9)

Aquí veremos que se mueve una zona de memoria, más específicamente el decriptor polimórfico. Luego genera una permutación de instrucciones, utilizando una tabla de Jumps.

Finalmente mueve de una zona de memoria a otra los Jumps generados. (ver Listado 10)



>>> Listado 9

```
        memmove(hVMMemory + vmPoly, _vm_poly_dec,
sizeof(_vm_poly_dec));
        genPermutation(condTab, 16);
        BYTE invCondTab[16];
        memmove(invCondTab, condTab, 16);
```

>>> Listado 10

```
        invPerm16(invCondTab);
        permutateJcc((WORD*)(hVMMemory + vmCodeStart + 17),
16, invCondTab);
        genPermutation(opcodeTab, VM_INSTR_COUNT);
        memmove(hVMMemory + vmOpcodeTab, opcodeTab,
VM_INSTR_COUNT);
        invPerm256(hVMMemory + vmOpcodeTab);
        *(WORD*)(hVMMemory + vmPrefix) = vm_instr_prefix;
```

>>> Listado 11

```
        int protSize = 0;
        for (int i = 0; i < itemsCnt; i++)
        {
                char temp[25];
                SendMessage(listBox, LB_GETTEXT, i,
(LPARAM)temp);
                temp[8] = 0;
                sscanf(temp, "%x", &items[i*2]);
                sscanf(temp + 11, "%x", &items[i*2 + 1]);
                items[i*2] -= inh->OptionalHeader.ImageBase;
                items[i*2 + 1] -= inh->OptionalHeader.Image-
Base;

                items2[i*2] = rva2raw(inh->FileHeader.Numbe-
rOfSections, ish, items[i*2]);
                if (items2[i*2] == 0xFFFFFFFF) ERROR2("Inva-
lid range start");
                items2[i*2 + 1] = items[i*2 + 1] -
items[i*2];
                int t = vm_protect(hInMem + items2[i*2],
items2[i*2 + 1], 0, items[i*2], (BYTE*)rel, inh->Optional-
Header.ImageBase);
                if (t == -1) ERROR2("[SIZE] Protection fai-
led.");
                protSize += t;
        }
```

Ahora, se invierte la permutación, en el código veremos varias funciones de estas, con buffers de 16 y 256 bytes. Así como también la función permutateJcc, que realiza una permutación de los saltos.

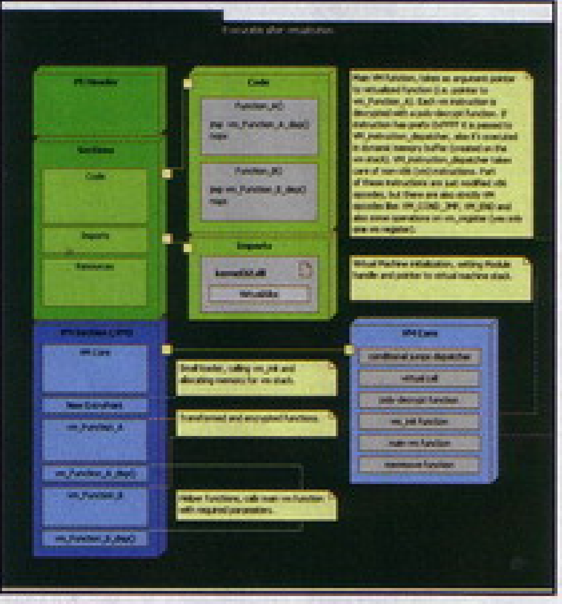
Podemos observar que como último parámetro a la función permutateJcc se le pasa la tabla de saltos invertidos generados anteriormente con la función invPerm16.

Después de esto, se copia una zona de memoria, para preparar la permutación de los códigos de operación.

```
        return vmSize;
}
```

Por último se retorna el tamaño de la VM creada. (ver Listado 11)

En el trozo de código de acá arriba, podemos ver, como va obteniendo cada ítem del listbox, es decir, cada zona a proteger que definimos anteriormente, analizando que éste rango sea válido, finalmente protege esas zonas, llamando a la función vm_protect, que como ya vimos, sabemos de que se trata.



x86.virt.after

Conclusión

Bien amigos, hemos llegado al final de este artículo especial, estudiando una de las protecciones más importantes de la era de la seguridad de software, contra el análisis de binarios y la piratería.

Tenemos que tener en mente, que las capacidades de este proyecto, recíen empiezan. Igualmente como mencioné anteriormente, posee sus errores, no suele andar bien y hay que arreglar varios aspectos que me parecieron un poco sucios y poco ortodoxos.

Simplemente se trata de una prueba de concepto, la cuál podemos intentar modificar, utilizar, re pensar e inclusive, crear a partir de esta, una nueva estrategia de VM, que pueda resolver de mejor manera lo que intenta resolver esta que empezamos a analizar.

Espero que les haya gustado.
Nos vemos en el próximo número.

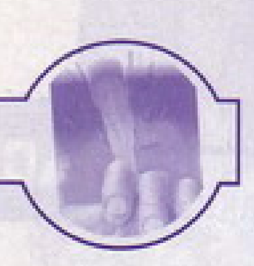
SparK
http://www.disidents.org
http://www.intrabytes.com
spark@disidents.org
arielrm@intrabytes.com



Borrado seguro de datos

Cuando queremos asegurarnos de que los datos están muertos... y enterrados

En plena época postindustrial, los enormes avances en las tecnologías de la información hicieron que, llegado un punto, el movimiento de la información fuera más rápido que el propio movimiento físico; momento que más tarde fue señalado como el nacimiento de la actual "era de la información". Desde entonces, y como actualmente ocurre, la información en ocasiones es más valiosa que el más precioso de los metales. Tus datos son codiciados por grandes empresas, spammers, ladrones, y hasta los propios gobiernos cuyo trabajo -en teoría- es protegerte. Y, sin embargo, la mayoría de la gente desconoce cómo proteger mínimamente esa pequeña parcela de privacidad que aún nos queda. ¿Crees que tus datos están a salvo borrándolos de tu disco duro? Ni mucho menos, ni muchísimo menos...



Bienvenidos seáis todos, queridos lectores. El borrado seguro de datos es uno de los campos más importantes dentro del panorama actual de la seguridad informática, y mucho más aún en el caso de almacenar datos sensibles o de terceras personas, pues la propia legislación te obliga a cumplir una serie de preceptos con respecto a los datos custodiados. ¿Y por qué hablo de borrado seguro? ¿Cual es, entonces, el borrado no seguro? Pues prácticamente cualquiera.

El mercado de la información

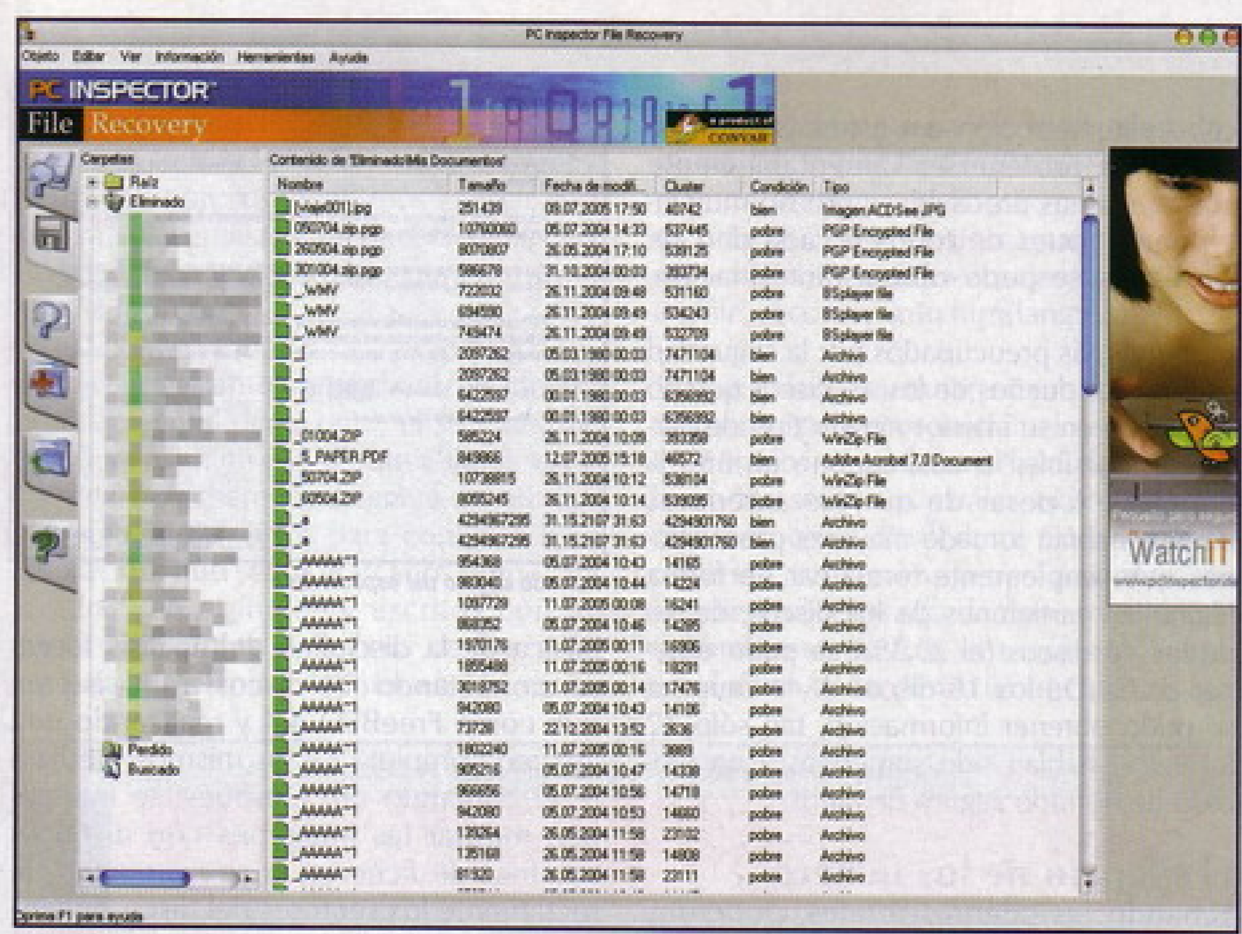
Los ordenadores de hoy en día poseen un potencial de almacenamiento de información masivo, y no es nada extraño encontrarse con que en un hogar cualquiera hay más de un terabyte de capacidad de almacenamiento de datos. Precisamente debido a este potencial, los canales y medios para el tratamiento de dicha información experimentan también un crecimiento similar y paralelo. Por ejemplo, las líneas de telecomunicaciones poseen cada vez un mayor ancho de banda y un menor coste (al menos fuera de España, claro), y los dispositivos de almacenamiento son cada vez mayores y más baratos.

Antes, cada ordenador poseía normalmente un único disco duro; mientras que hoy en día no sólo posee varios discos internos, sino que además es habitual la utilización de medios externos de almacenamiento masivo con capacidades mayores incluso que la de los primeros. Y, por supuesto, el mercado de segunda mano para este tipo de dispositivos también está en auge: sólo hay que echar un vistazo a páginas de venta por Internet (como eBay) para ver la gran cantidad de discos duros que se venden cada pocos minutos.

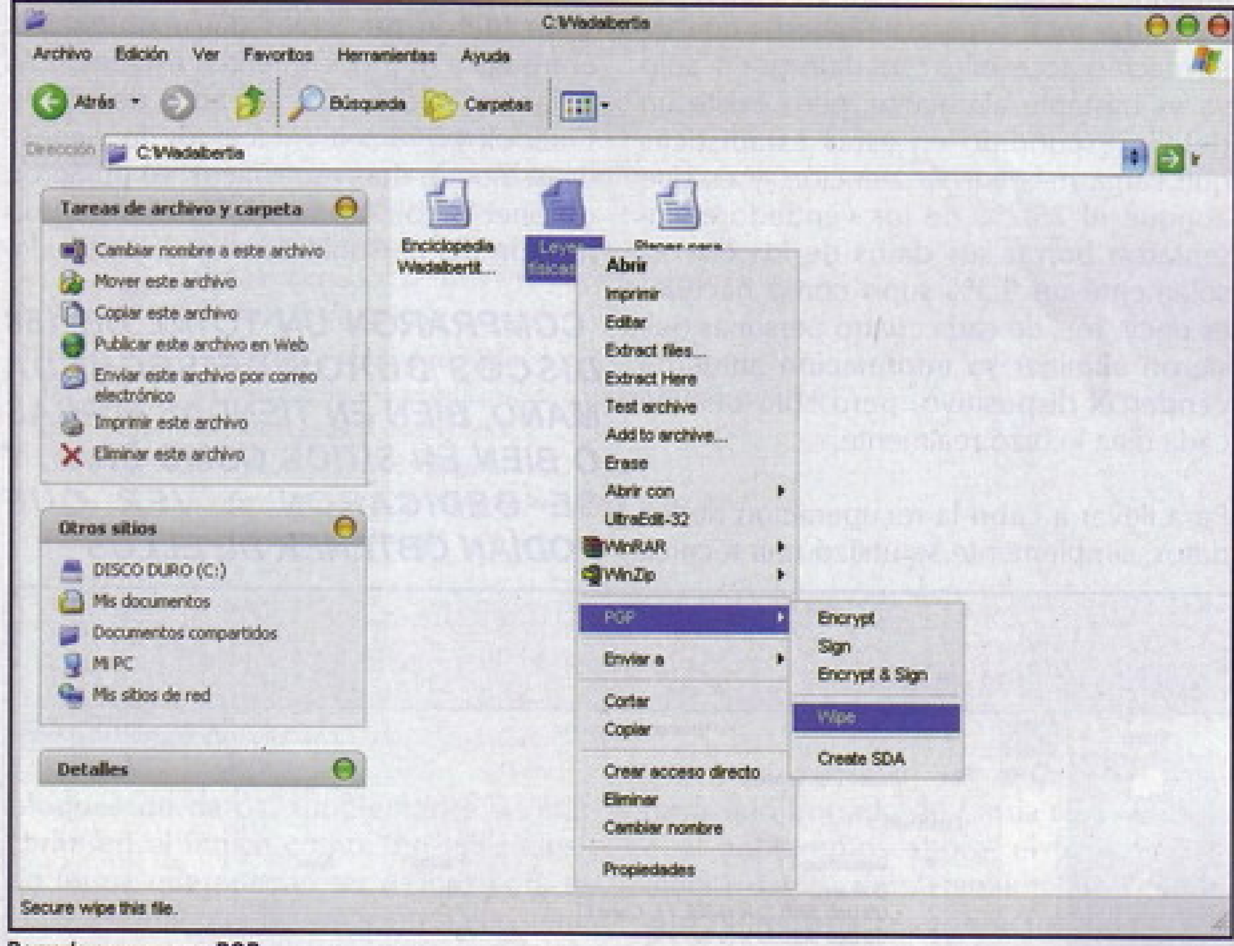
Personalmente, prefiero comprar los dispositivos de almacenamiento nuevos, y nunca me he deshecho de ninguno de los que he tenido, pues prefiero guardarlos aún cuando no los utilice. Pero sí conozco gente que ha comprado discos duros de segunda mano, o equipos portátiles con el disco duro original, etc. Y, aunque parezca mentira, vender discos duros de segunda mano puede resultar peligroso.

Cuando los datos no mueren

Hace ya unos cuántos añitos, dos estudiantes del Instituto Tecnológico de Massachusetts realizaron un interesante estudio sobre la venta de discos duros usados. Compraron un total de 158 discos duros de segunda mano, bien en tiendas físicas o bien en sistios de compra por Internet como eBay, y se dedicaron a ver qué podían obtener de ellos. Como



Visor de ficheros eliminados



Borrado seguro con PGP

en todo estudio estadístico que se precie, lo primero que se hizo fue eliminar de la muestra aquellos datos erróneos, y es que sólo 129 de los 158 discos estaban en condiciones de funcionamiento. Para que te fíes de la compra de segunda mano en según qué casos...

El mayor nivel de desprotección lo encontraron en los 32 discos que contenían particiones accesibles con datos almacenados en ellas directamente, lo cual supone que el 24,8% de la gente no se molestó ni en borrar los datos. Por supuesto, no hace falta ser ningún hacker para recuperar datos de discos en semejantes condiciones.

Un poco más precavidos demostraron ser los dueños de los 51 discos que, aún conteniendo particiones accesibles, habían sido formateados previamente a su venta. No está mal, pues indica que un 39,5% de los vendedores se preocuparon por el posible destino de sus datos y llevaron a

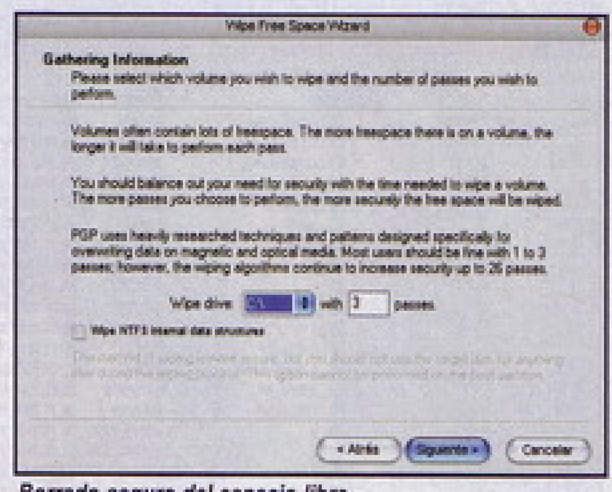
cabo alguna acción -en este caso, formatear- para protegerse. Lamentablemente eran personas precavidas pero no muy informadas, pues de todos y cada uno de los discos se pudo obtener información.

Bastante más preocupados por la seguridad estaban los dueños de los 46 discos que no contenían en su interior ningún tipo de partición accesible, lo cual supone un 35,7% del total. A pesar de que los anteriores dueños habían tomado mayores precauciones que simplemente formatear de forma lógica las particiones de los discos, de 30 de los 46 discos (el 23,3%) se pudo obtener datos. De los 16 discos de los que no se pudo obtener información, tan sólo 12 (el 9,3%) habían sido sometidos a un proceso de borrado seguro de datos.

El silencio de los ficheros

Echando las cuentas totales, podemos comprobar que en el 87,6% de los discos adquiridos pudieron encontrarse -bien sea de forma total o parcial- ficheros con información accesible. Este dato por sí sólo ya es bastante alarmante, pero existe un detalle escondido en estas estadísticas que llama más aún la atención, y es que aunque el 75,2% de los vendedores intentaron borrar sus datos de los discos, solamente un 9,3% supo cómo hacerlo; es decir, tres de cada cuatro personas quisieron eliminar su información antes de vender el dispositivo, pero sólo una de cada diez lo hizo realmente.

Para llevar a cabo la recuperación de los datos, simplemente se utilizó una técnica



Borrado seguro del espacio libre

básica de la disciplina del análisis forense, conectando los discos a un sistema que corría FreeBSD 4.4 y realizando una imagen completa de los mismos mediante el comando dd. Después, se intentaban montar las imágenes con distintos sistemas de ficheros, o se rastreaban directamente los sectores del disco en busca de información.

Y no fueron pocos los datos obtenidos, entre ellos 675 documentos escritos, 274 hojas de cálculo, 20 volcados de correo Outlook y 566 presentaciones de diapositivas. Siendo más específicos, se pudieron obtener datos tan sensibles como información del personal de una empresa, documentos médicos, documentos de un hospital infantil, cartas personales, pornografía como para llenar otro Internet...

COMPRARON UN TOTAL DE 158 DISCOS DUROS DE SEGUNDA MANO, BIEN EN TIENDAS FÍSICAS O BIEN EN SITIOS COMO EBAY, Y SE DEDICARON A VER QUÉ PODÍAN OBTENER DE ELLOS

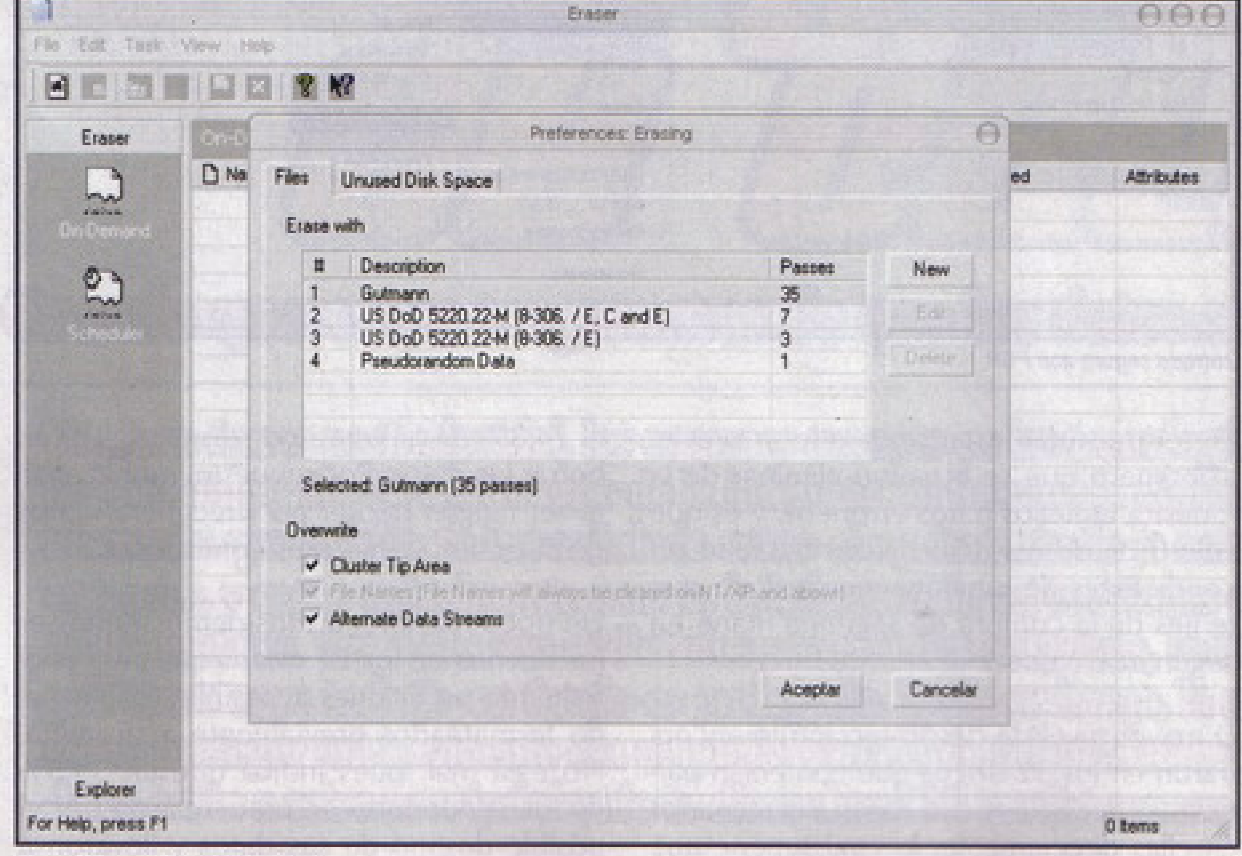
Pero se quiso ir más allá, y se buscó información de tarjetas de crédito en todos los discos. Rastreando los ficheros, se encontraron números válidos en 42 discos (el 32,6%), existiendo respectivamente más de 2800 y 3700 en dos únicos discos. El primero de ellos, tras un análisis más minucioso, resultó ser un disco duro procedente de un cajero automático; mientras que el segundo no llegó a averiguarse, si bien 3700 números de tarjeta de crédito en un fichero de log huelen a delincuente electrónico.

Si ya es problemático que se dé esta situación en el ámbito particular, cuando se da en el empresarial o gubernamental, existiendo leyes como la LOPD que regulan el tratamiento de ficheros con información protegida, no sólo hablamos de los datos, sino de responsabilidades legales bastante serias.

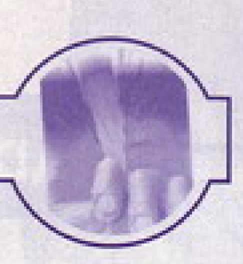
La culpa es de Faraday

Actualmente estamos comenzando a leer noticias sobre la comercialización de los primeros discos duros de estado sólido, basados en la misma tecnología que las memorias USB o las tarjetas de memoria que actualmente podemos encontrar en casi cualquier aparato electrónico. No es una tecnología nueva, pues lleva utilizándose en la industria militar desde los años setenta (ya sabemos cómo se las gasta el tío Sam), pero sí ha visto abaratado su coste lo suficiente como para que empiece a resultar rentable su uso comercial. Para que os hagáis una idea, Dell comercializa una gama de portátiles (la XPS) que puede adquirirse sustituyendo el disco duro SATA de 120 Gb por un disco de estado sólido (SSD) de 64 Gb, suponiendo esta sustitución un incremento del precio de 1000 dólares, en el caso concreto del modelo XPS M1330. Imaginad cuánta pasta costaría uno de los discos montados en un avión de combate de hace treinta años...

No voy a engañar a nadie, todo (o al menos la gran mayoría) lo que os voy a contar no es aplicable cuando se utilizan estos discos, así que cuando los ordenadores incorporen discos SSD de forma habitual, la problemática del borrado seguro de datos muy probablemente se irá al garete. Pero no será lo único que deberá cambiar: los planificadores de entrada/salida de los sistemas operativos, la práctica totalidad del



Algoritmos de borrado seguro



sistema de gestión de peticiones de las bases de datos, los sistemas de ficheros actuales... en fin, posiblemente el borrado seguro de datos será el menor de los problemas, máxime cuando será uno de los pocos que se solucionará solito.

¿Y la culpa de quién es? Yo se la he echado injustamente al pobre Faraday, aunque en realidad es del electromagnetismo. Como el primero murió hace mucho, y el segundo es una rama de la física, será mejor que lo veamos con más detenimiento. Esencialmente, los discos actuales no han cambiado demasiado desde los albores de la informática; y de hecho su base física es prácticamente la misma que la de las cintas de datos. ¿Alguien se acuerda de las cintas de casete? Pues es casi lo mismo.

Los discos duros modernos tienen en su interior un cierto número de discos, cada uno de los cuales está recubierto por una aleación metálica ferromagnética. Debido a su naturaleza electromagnética, dichos materiales pueden magnetizarse de diversas formas aplicando unos campos en su entorno. No es el momento de explicar al detalle el funcionamiento interno de los discos duros, ni mucho menos de dar una clase de física; para ambas cosas podéis recurrir a la Wikipedia o cualquier otra página temática. Baste decir que esta propiedad es aprovechada para codificar la información en la superficie de los mencionados discos, magnetizándola de una determinada forma; y detectando dicha magnetización para leer los datos almacenados.

¡Zas! En todo el sistema de ficheros

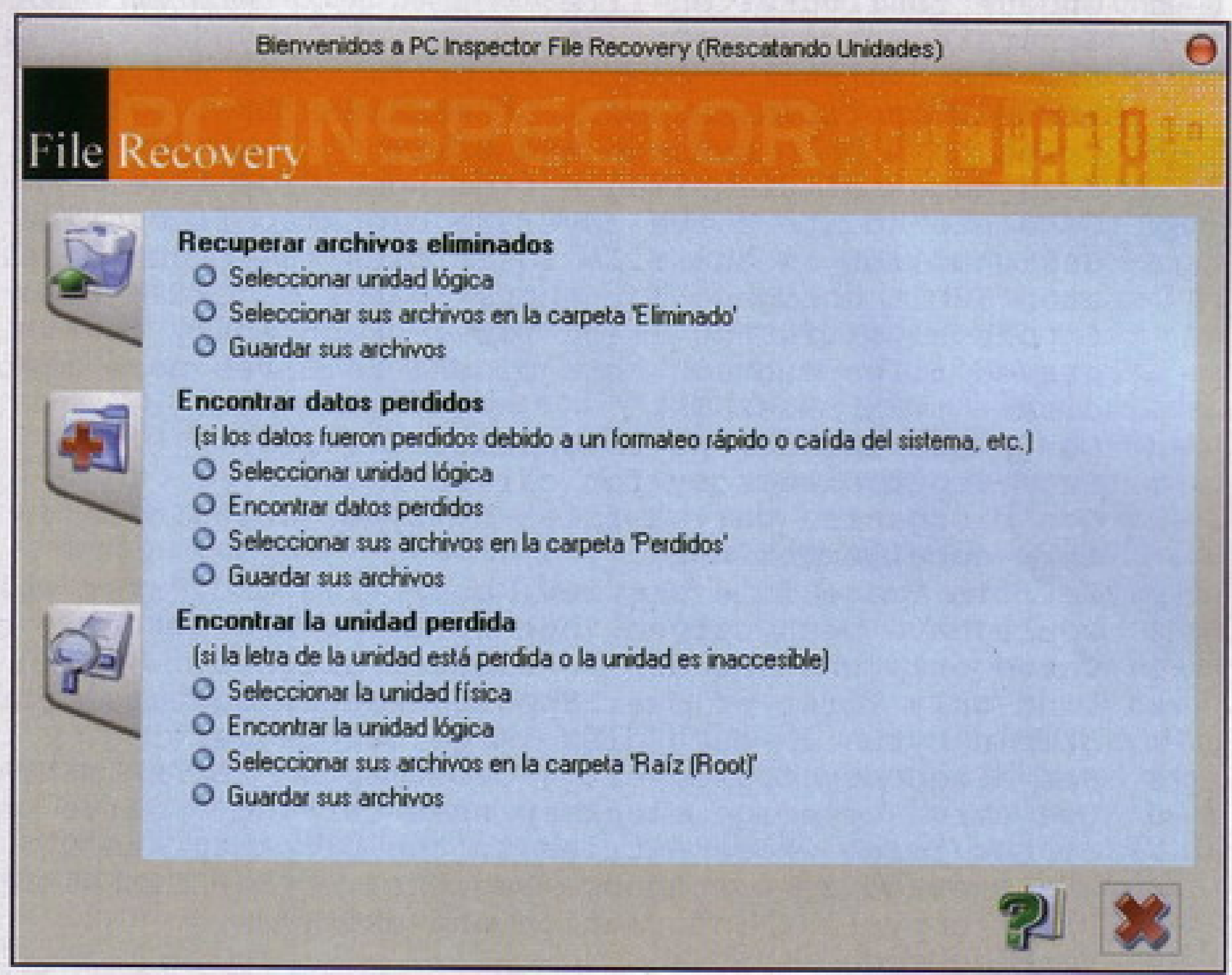
Seguramente habréis observado en multitud de ocasiones cómo un fichero que tarda un tiempo significativo en escribirse en el disco, es borrado en apenas una fracción de segundo sin pestañear. ¿Os habéis preguntado alguna vez por qué ocurre esto? Pues esta increíble velocidad de borrado es debida a un truquito que usan la mayoría de los sistemas de ficheros y que consiste en algo tan simple como no borrar lo que se le pide que borre. Suena raro, pero así es.

Todos los sistemas de ficheros poseen un elemento denominado "índice", que funciona de la misma forma que el índice de una obra literaria. Si en un libro consultamos el índice en busca de la página en la que se encuentra un determinado contenido, en un sistema de ficheros lo consultamos en busca del bloque en el que se encuentra una determinada información. Cada sistema de ficheros (FAT, NTFS, EFS, ext3, JFS, ReiserFS, HFS...) usará su sistema de índice, con sus algoritmos asociados, y tendrá sus ventajas e inconvenientes, pero todos ellos funcionan básicamente de la misma forma.

Cuando escribimos un fichero de tamaño arbitrario en el disco duro, el sistema operativo consultará los bloques libres en el sistema de ficheros, y asignará un número determinado de ellos para contener la información, que serán marcados como "utilizados" en el índice y escritos con los datos pertinentes. A la hora de borrarlos, en lugar de eliminar la información de los bloques de datos, simplemente se marcarán en el índice como "no utilizados", de forma que puedan ser usados para escribir encima otra información si el sistema operativo así lo solicita. Evidentemente, mientras dicha información no sea sobrescrita, los datos originales que fueron "borrados" permanecerán físicamente en el disco duro.

Para comprobar de forma práctica cómo, debido a esta particularidad de los sistemas de ficheros, se puede obtener información que teóricamente había sido eliminada de un sistema, simplemente debemos utilizar algún software de recuperación de datos de los muchísimos existentes en el mercado. Para plataformas Windows, una buena elección es el programa PC Inspector File Recovery, que es gratuito (aunque no libre) y muy sencillo de utilizar. Podemos descargarlo de la página oficial: http://www.pcinspector.de/Sites/file_recovery/info.htm?language=1.

Tras instalar y ejecutar el programa, simplemente debemos iniciar el asistente incorporado para ver una lista de archivos borrados sobre los cuales existe información aún en el disco duro. Como podréis observar en las imágenes adjuntas, dependiendo del grado de conservación del fichero, será posible obtener más o menos información de él. En el caso de que haya sido borrado de forma segura -de lo cual hablaremos ahora- el fichero contendrá datos completamente sin sentido, aún cuando la recuperación haya sido lanzada tras el borrado del archivo, y sin que haya tenido lugar ninguna otra operación de escritura en disco.



Diálogo de rescate de unidades

Para sistemas Linux, un programa bastante interesante para analizar imágenes de disco (que pueden ser obtenidas con el mismo método que utilizaron en el estudio del MIT) es scalpel. (ver Listado 1)

¡Zas! En todo el magnetismo

A grandes males, grandes remedios. Si sabemos que la información contenida en el disco no será eliminada realmente hasta

>>> Listado 1

```
master@blingdenstone:~$ scalpel -h
Scalpel version 1.60
Written by Golden G. Richard III, based on Foremost 0.69.
Carves files from a disk image based on file headers and footers.

Usage: scalpel [-b] [-c <config file>] [-d] [-h|V] [-i <file>]
          [-m blocksize] [-n] [-o <outputdir>] [-O num] [-q clustersize]
          [-r] [-s num] [-t <blockmap file>] [-u] [-v]
          <imgfile> [<imgfile>] ...

-b  Carve files even if defined footers aren't discovered within
    maximum carve size for file type [foremost 0.69 compat mode].
-c  Choose configuration file.
-d  Generate header/footer database; will bypass certain optimizations
    and discover all footers, so performance suffers.  Doesn't affect
    the set of files carved.  **EXPERIMENTAL**
-h  Print this help message and exit.
-i  Read names of disk images from specified file.
-m  Generate/update carve coverage blockmap file.  The first 32bit
    unsigned int in the file identifies the block size. Thereafter
    each 32bit unsigned int entry in the blockmap file corresponds
    to one block in the image file.  Each entry counts how many
    carved files contain this block. Requires more memory and
    disk.  **EXPERIMENTAL**
-n  Don't add extensions to extracted files.
-o  Set output directory for carved files.
-O  Don't organize carved files by type. Default is to organize carved files
    into subdirectories.
-p  Perform image file preview; audit log indicates which files
    would have been carved, but no files are actually carved.
-q  Carve only when header is cluster-aligned.
-r  Find only first of overlapping headers/footers [foremost 0.69 compat mode].
-s  Skip n bytes in each disk image before carving.
-t  Set directory for coverage blockmap.  **EXPERIMENTAL**
-u  Use carve coverage blockmap when carving.  Carve only sections
    of the image whose entries in the blockmap are 0.  These areas
    are treated as contiguous regions.  **EXPERIMENTAL**
-V  Print copyright information and exit.
-v  Verbose mode.
master@blingdenstone:~$
```

que sea sobrescrita, simplemente deberíamos sobreescribirla y punto, ¿no? El problema está en que, en el nivel de la aplicación, absolutamente nada nos garantiza dónde le va a apetecer al sistema operativo escribir nuestros datos. Un documento de texto de OpenOffice.org, por poner un ejemplo, guarda una copia temporal durante la edición para prevenir posibles pérdidas en caso de caída del sistema, así que sobrescribir el texto no nos puede garantizar el borrado de los datos.

Pues nada, siguiente nivel: formateamos el disco duro. Lamentablemente tampoco supone una solución, como habéis podido leer al principio del artículo en relación con el estudio del MIT. El "formateo rápido" de Windows es otro de esos maravillosos términos absurdos, engañosos y contradictorios acuñados por la gente de Redmond (como el "modo a prueba de fallos de Windows"), pues un formateo no puede ser rápido por definición.

Cuando aplicamos un "formateo rápido" a un disco, únicamente se elimina la información del índice para que parezca que no hay ningún fichero en el disco, pero la información no se toca; por lo que sería equivalente a borrar todos los ficheros. Sin embargo, un formateo físico sí que sobrescribe toda la información contenida en sus bloques de datos, estableciendo su valor a nulo.

Pero el electromagnetismo no perdona, de forma que dos elementos magnetizados de forma diferente a los que apliquemos una misma excitación electromagnética, darán lugar a dos campos magnéticos distintos. Dado el orden de magnitud de los campos utilizados en los discos duros, la diferencia será minúscula. Pero existirá. Y sólo se necesitan los suficientes recursos económicos como para poder desplegar los medios necesarios para que esas ínfimas diferencias se transformen en resulta-

dos. Puede que tu prima pequeña perdiera el interés, pero nuevamente el tío Sam sólo necesita los motivos, porque la pasta la tiene y el tiempo lo compra con ella.

Vayamos un paso más allá. Si sobrescribir toda la información con un mismo dato no funciona, hagámoslo con datos diferentes. Dado que si seguimos un patrón a la hora de generar los datos que usaremos para sobrescribir la información, nos encontraremos con el mismo problema que ya teníamos; será preciso que los datos no sigan ningún patrón, o lo que es lo mismo, que sean aleatorios.

Determinismo y aleatoriedad

Nuevamente nos encontramos con una piedrecita en el camino: ¿cómo generar los datos aleatorios? Para cualquiera de nosotros es tan sencillo como utilizar cualquiera de los múltiples sistemas caóticos que nos rodean, por ejemplo, lanzando dados al aire y dejando que la física haga el resto. Pero un ordenador es un sistema determinista, o lo que es lo mismo, a partir de una misma entrada y aplicando el mismo algoritmo, siempre obtendrá una misma salida. Esta circunstancia, que tan útil nos resulta a la hora de ejecutar aplicaciones, nos molesta bastante si lo que queremos es obtener datos aleatorios.

Pero no todo está perdido, pues aunque no es posible obtener datos aleatorios con un ordenador, sí que se pueden obtener datos pseudoaleatorios con los denominados PRNG (Pseudorandom Number Generator), que se sirven de la entropía externa del sistema para generar datos con un grado de aleatoriedad casi total. Esta entropía puede ser captada de la interacción con el usuario (mediante el movimiento del ratón o el tecleo), de las interacciones del sistema (como el flujo de red) o por medio de otros métodos.

También pueden obtenerse números aleatorios prácticamente reales con hardware dedicado (generadores de números aleatorios por hardware), que basándose en efectos físicos teóricamente impredecibles (como el ruido térmico, el fenómeno fotoeléctrico o fenómenos cuánticos) son capaces de obtener, mediante un transductor, una lectura del estado de dicho proceso representada como información digital.

ISAAC el impredecible

La generación de números pseudoaleatorios y la criptografía son dos disciplinas que tienen mucho en común, y que en multitud de ocasiones entrecruzan sus caminos: la criptografía se sirve de la generación de números pseudoaleatorios, por ejemplo, en los procesos de generación de claves de cifrado; mientras que los PRNG se sirven de algoritmos muy similares a los empleados en criptografía para generar sus valores de salida.

Uno de los generadores de números pseudoaleatorios más conocidos y utilizados es ISAAC (Indirection, Shift, Accumulate, Add and Count), ideado en 1996 por Robert J. Jenkins e inspirado en el PRNG del popular algoritmo de cifrado RC4 de Ron Rivest (utilizado, entre otros, en el proceso de cifrado WEP). En 2001, Marina Pudovkina presentó un estudio sobre un ataque criptoanalítico que reducía la complejidad a la hora de predecir salidas de las 10^2466 iteraciones esperadas a tan sólo 4,67 * 10^1240, aunque dicha complejidad sigue siendo inabordable con la potencia de cálculo actual.

Más tarde, en 2006, Jean-Philippe Aumasson presentó como descubrimiento una serie de "estados débiles" inspirándose en una debilidad conocida del algoritmo RC4, en cuyo PRNG se basa ISAAC, y propuso una mejora del algoritmo (ISAAC+); si bien había ciertos errores en la investigación, comenzando por que el algoritmo ISAAC que usaron no estaba implementado correctamente. Actualmente, ISAAC sigue considerándose seguro y es ampliamente utilizado.

Destruyendo datos

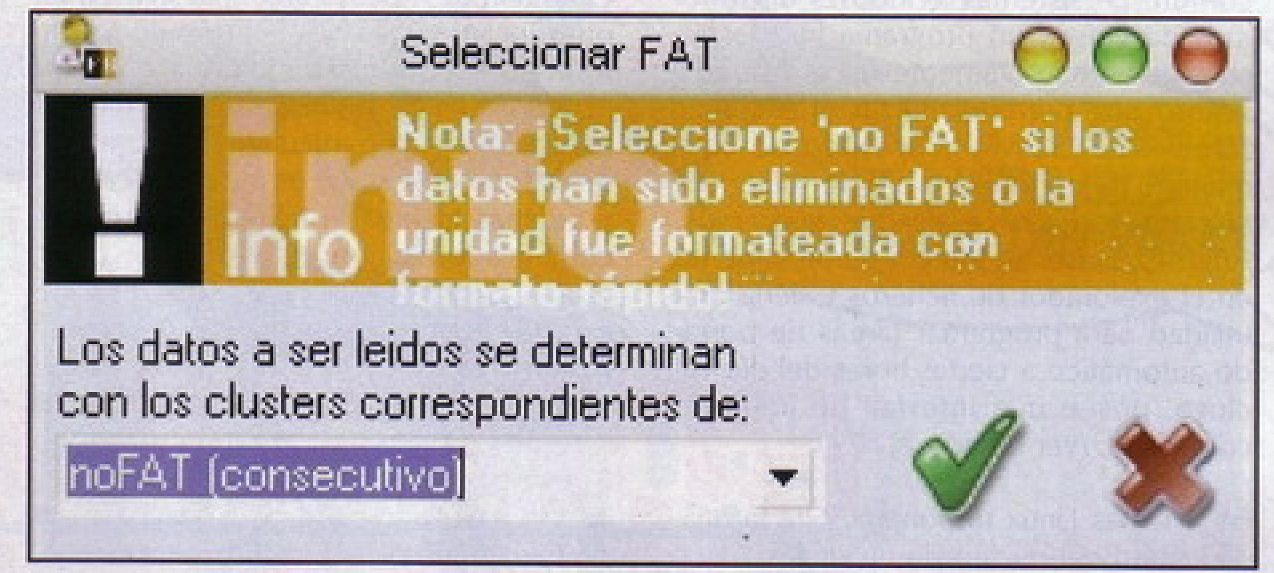
Usando como base ISAAC (o cualquier otro PRNG), se construyen los llamados algoritmos de borrado seguro, que se sirven de ciertas primitivas del sistema operativo para acceso a ficheros, de forma que pueden sobrescribir la información real almacenada en los bloques del disco duro.

Prácticamente todos los algoritmos de borrado seguro de datos más utilizados cumplen el estándar "DoD 5220.22-M" del manual de operaciones del programa de seguridad industrial nacional (NISPOM) de Estados Unidos. O al menos lo cumplían hasta hace poco, pues desde noviembre de 2007 el departamento de defensa de yankilandia no acepta la sobrescritura de datos como un método aceptable de eliminación de ficheros, validando únicamente los procesos de desmagnetización o destrucción física.

Como ejemplo, el sistema de borrado seguro de datos de PGP excede la seguridad exigida hasta hace unos meses por dicho estándar cuando se configura en tres o más pasadas de borrado. En las opciones de configuración de PGP se podrá ajustar dicho número de pasadas, pero es importante tener en cuenta que cuanto mayor sea el número de éstas, más durará el proceso de borrado. Para utilizar el borrado seguro de PGP, únicamente debemos seleccionar la opción "Wipe" en el submenú PGP del menú contextual que surge al hacer click derecho sobre un fichero en el explorador. Otra opción interesante de PGP es el borrado seguro del espacio libre en disco, pues existe una gran cantidad de datos en todas las áreas del disco marcadas como "vacías" por el sistema de ficheros.

El método Gutmann

Pero posiblemente el algoritmo más famoso de borrado seguro es el conocido como "método Gutmann", propuesto



Configuración del cluster

>>> Listado 2

```
C:\Archivos de programa\Eraser>eraserd /?
Eraser 5.6 for DOS. Free Software.
Copyright 2002 Garrett Trant. (http://www.heidi.ie/eraser/)
Usage:
 eraserd [ Data] [ -passes passes] [ -silent]
 Data:
   -file       data [ -nodel]
   -folder     data [ -subfolders] [ -keepfolder]
   -disk       drive: [ -notips]
   -allfiles drive:
 Parameters:
   -file           Erase file(s) (wildcards allowed)
    -nodel            Do not delete file(s) after erasing
   -folder          Erase all files in the folder
    -subfolders       Include subfolders
    -keepfolder       Do not delete the folder
   -disk            Erase unused space on the drive
    -notips           Do not erase cluster tip area
   -allfiles        Erase all files on a drive
   -passes            Number of overwriting passes (default 1)
   -silent          Nothing to standard output
C:\Archivos de programa\Eraser>
```

por Peter Gutmann en su artículo "Secure Deletion of Data from Magnetic and Solid-State Memory". Este algoritmo se basa en 35 iteraciones en las que se sobrescribe la información almacenada en el disco. Las cuatro primeras iteraciones, así como las cuatro últimas, son realizadas con datos pseudoaleatorios obtenidos con un PRNG (típicamente ISAAC), mientras que las 27 iteraciones centrales son realizadas con una serie de patrones prefijados, ideadas para eliminar todo rastro de la información independientemente de los datos que contuviera el disco con anterioridad, y siendo éstas aplicadas en orden aleatorio.

Este algoritmo es implementado por multitud de programas, pudiendo encontrar software libre de calidad y sencillo de utilizar para cualquier plataforma de uso común. En sistemas Windows disponemos de Eraser, un programa libre especializado exclusivamente en el borrado seguro que permite utilizar el estándar "DoD 5220.22-M", el método de Gutmann, o definir nuestro propio método a la carta, todo lo bestia que queramos. Además, Eraser se integra perfectamente en el explorador de ficheros y tiene una utilidad para programar tareas de borrado automático a ciertas horas del día. Incluso, posee una interfaz de línea de comandos: (ver Listado 2)

En sistemas Linux disponemos de la utilidad shred del núcleo de utilidades GNU, que sobrescribe la información en el interior de un fichero. Prácticamente cualquier sistema Linux dispone de la aplicación, y podemos probarla simplemente ejecutando los siguientes comandos:

```
master@blingdenstone:~$ echo
hola > prueba.txt
master@blingdenstone:~$ cat
prueba.txt
hola
master@blingdenstone:~$ shred
prueba.txt
master@blingdenstone:~$ cat
prueba.txt

[ salida del fichero elimina-
do]

master@blingdenstone:~$
```

Otra utilidad que implementa el método Gutmann es wipe. Es algo más avanzada, pues incluye opciones como recorrer de forma recursiva los directorios o definir la fuente de la semilla de aleatoriedad utilizada, y a mí particularmente me gusta más. Su utilización es igual de sencilla, y además elimina el fichero tras sobrescribir la información:

```
master@blingdenstone:~$ wipe
prueba.txt
Okay to WIPE 1 regular file ?
(Yes/No) yes
Operation finished.
1 file wiped and 0 special
files ignored in 0 directo-
ries, 0 symlinks removed but
not followed, 0 errors occu-
red.
master@blingdenstone:~$
```

Un buen método para comprender la importancia de estos algoritmos de borrado seguro de datos es usar distintos sistemas de ficheros para crear y borrar mediante diversos métodos varios archivos, para posteriormente tratar de recuperarlos por medio de alguna de las utilidades comentadas.

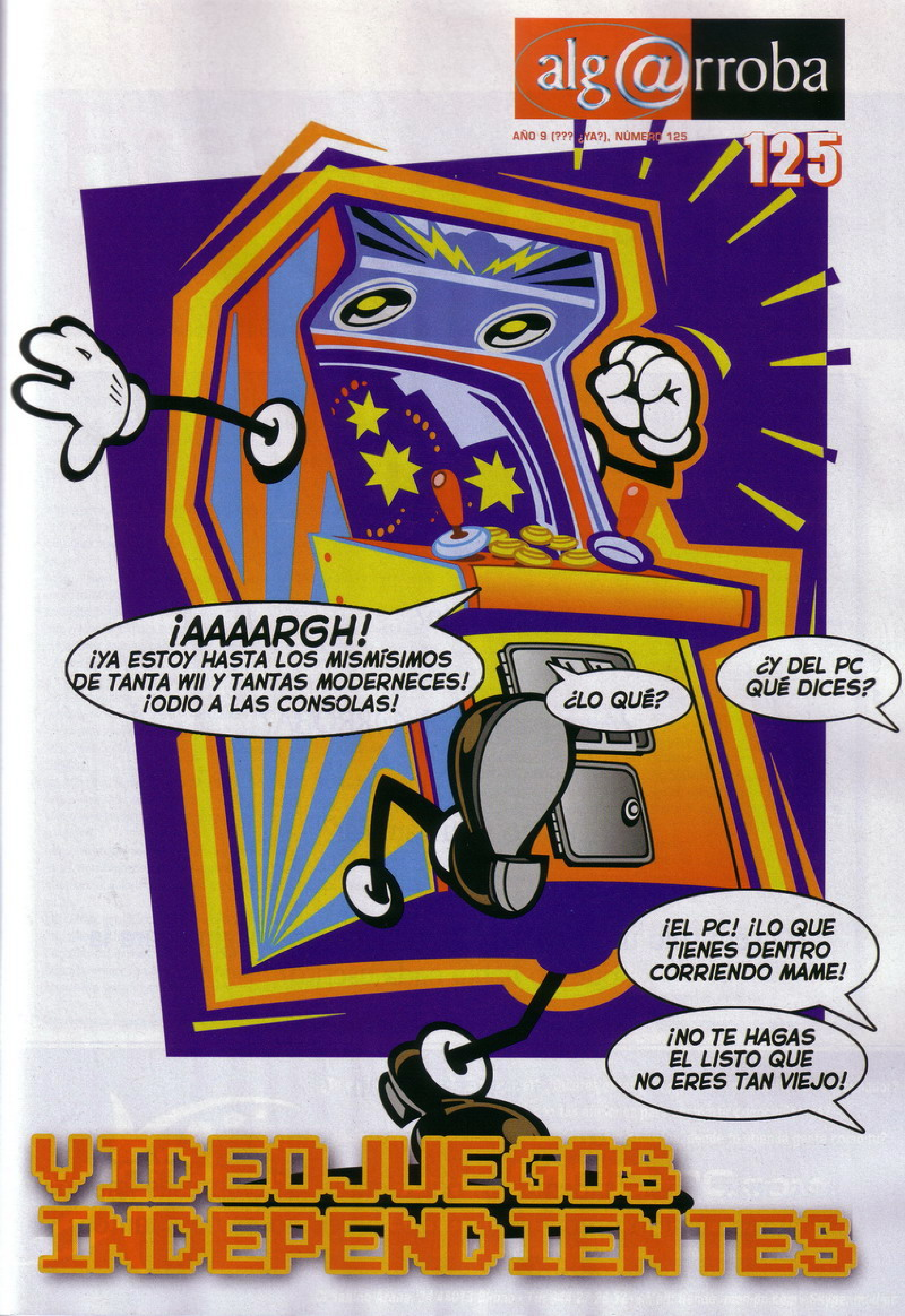
Concluyendo

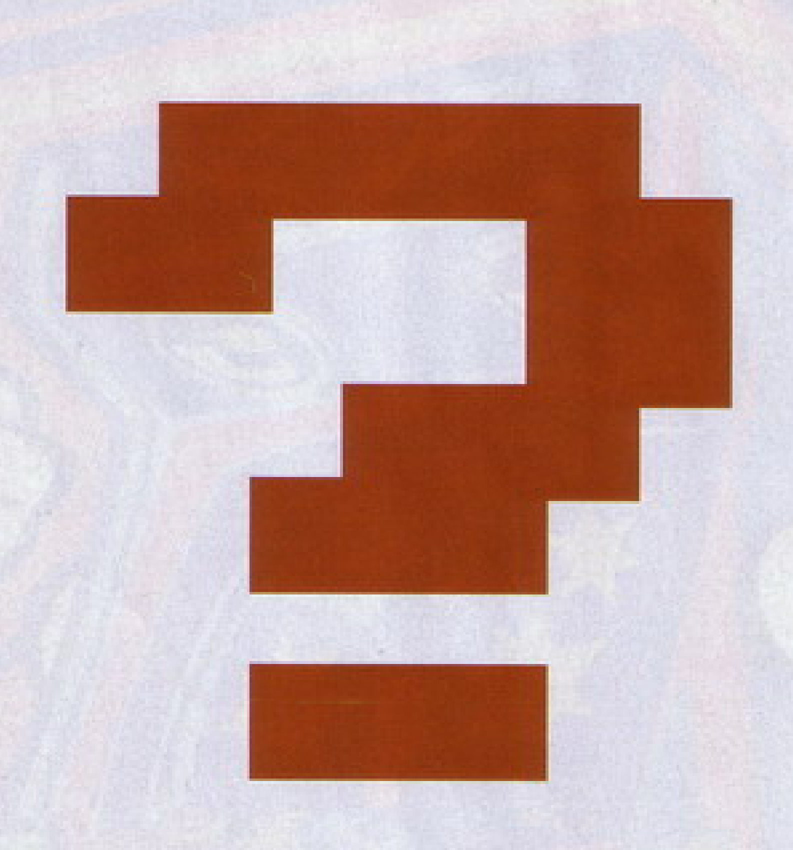
Como podéis ver, los medios para utilizar sistemas de borrado seguro de datos de nivel gubernamental están en nuestras manos, y son en su mayoría software libre. Ahora que comprendéis la importancia de este proceso y cómo llevarlo a cabo, espero que entre vuestras costumbres pase a estar la de borrar de forma segura de vuestros discos duros todo fichero con datos sensibles o importantes.

Combinar estas técnicas con la criptografía puede aumentar enormemente el nivel de seguridad de vuestros sistemas. Por ejemplo, GnuPG y TrueCrypt (del que hablamos hace un par de meses en esta misma revista) pueden ser opciones muy interesantes a tener en cuenta.

¡Hasta otra!

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com


alg@rroba
AÑO 9 (??? ¿YA?), NÚMERO 125
125
¡AAAARGH! ¡YA ESTOY HASTA LOS MISMÍSIMOS DE TANTA WII Y TANTAS MODERNECES! ¡ODIO A LAS CONSOLAS!
¿LO QUÉ?
¿Y DEL PC QUÉ DICES?
¡EL PC! ¡LO QUE TIENES DENTRO CORRIENDO MAME!
¡NO TE HAGAS EL LISTO QUE NO ERES TAN VIEJO!
VIDEOJUEGOS INDEPENDIENTES



¿Ein?

¿Algo pasa en alg@RROBA?

¿Algo va a cambiar?

¿O será solo una excusa para rellenar una página para la que no había nada escrito?

A esperar tocan.

Juas, juas. Ahora sabemos lo que sienten las empresas importantes cuando preparan algo que luego no es para tanto.

Freak Domain

Los Dioses deben estar locos

¡Desparrame de fotoblogs!

En este desgobierno que es alg@rroba este mes, hemos querido poner un poco de calma. Y no hemos podido, así que para empeorar las cosas, batería enorrrrme de fotoblogs para combatir el frío con nuestras propias armas. Ejem.

http://www.doubleviking.com/international-babe-of-the-day-bar-refaeli-6611-p.html
http://ass.bodsforthemods.com/galleries/2007/11/met_art_presents_iga/index.php
http://www.bodyinmind.com/cgi-bin/BIMP3_gallery.cgi?vercode=15080:9804000000668375
http://fhg.bcash4you.com/p4e/fhg-rotator/?1099293
http://www.labatidora.net/gallery.php?galeria=peter131207oxana&idi=ing
http://www.galleries.badgirlsblog.com/albums/sophialucci/sophia_lucci_black_desire.html
http://girls.twistys.com/preview/totm/12-2007/something_cozy_by_the_fire_green/?t6/revs=tccoolio/
http://www.hasbabes.com/gallery/felicity_fey/room/
http://www.glam0ur.com/gals/naked_nina/index.php
http://www.galleries.coolios.net/eva/Adriana_in_Golden_Shadows_by_Evas_Garden/
http://hosted.femjoy.com/galleries/111815_uxj235_uuj845/?affid=809211
http://www.fritzryan.com/hostedpics/jana_f11/coolio.html
http://www.kindgirls.com/gal.php?dir=jula_9388&nom=Jula&num=12&pub=hegre
http://www.dailyniner.com/adelestephens1.shtml
http://www.bigboobsalert.com/gabrielle-xxcel.php
http://ass.bodsforthemods.com/galleries/2007/12/digital_desire_brenda/index.php
http://fresonmagic.com/fotos7/sarahcabania.htm
http://hosted.femjoy.com/galleries/111762_xki038_xii648/?affid=809211
http://hosted.met-art.com/Full_met-art_err_161_818/?pa=637705
http://dailyniner.com/ericaellyson1.shtml?
http://www.yourdirtymind.com/iga-means-business.html?
http://bustynudebabes.com/galleries/DDFBusty/2007/11/Gabriela/index.html?
http://www.babesdump.net/metart_16/5285/uliana
http://nude.hu/ginger-jolie-pics
http://babe-envy.com/pd_martina.html?
http://www.yourlust.com/galleries/katie-fey/28fca3/index.shtml?
http://sexykittenporn.com/jessica/?
http://www.babeskickass.com/content/Lux_Kassidy/
http://www.babes2you.com/lisa-marie
http://www.morazzia.com/playboy-galleries/2649/kasi-woodall.html?
http://galleries.pmates.com/galleries/ddgirls/2007-02/ddg_dreamgirls_2800_natalia_cruze/
http://www.foxhq.com/dina-top-of-the-morning/
http://www.m-u-s-e.org/hosted/55-ok88jmey.php
http://www.fantasybabes.info/2007/02/16/sultry-playboy-playmate-caramichelle/
http://novoporn.com/courtney-culkin4?
http://www.dailyhotmodels.com/galleries/ginger_jolie_pornstars/digital_desire.php?
http://nude.hu/black-nighty-boobs
http://z0d.com/scarlettkaleian.shtml
http://www.babeunion.com/gallery/ashley-lynn/
http://dachix.com/babe-800_Divini+Rae.html
http://hosted.goldinaraw.com/jam1_20122007/index.php?pa=1632136
http://babeskickass.com/go.php?Id=asredas.com&Out=http%3A%2F%2Fwww.asredas.com%2Fgallery%2F540%2FView_Porn_Starts%2FDamn_Hot_Beauty_Sandra_F%2F
http://www.100bucksbabes.com/sweet-krissy
http://www.babeskickass.com/content/Klara_in_black_lingerie/
http://houseofmodels.com/galleries/1byday/tsi/0001/index.php?
http://www.galleries.coolios.net/twistys/Monika_Vesela_in_black_lingerie_by_Twistys/
http://click.playboygirls.com/gallhit.php?125489,554,2,1,0
http://www.nextdoormania.com/met-art-scarlett-fishnet.php
http://www.lettherebeporn.com/galleries/2008/1/playboy_presents_jo_garcia/index.php
http://galleries.danni.com/121716/photos/sammie_rhodes8/

FRIKI GADGET

Las penas con pan son manos, pero si encima en vez de pan tenemos cacharritos ya es el despiporre. ¿Quién quiere amor, habiendo gadgets?





Odio a tus hijos, que conste

Si los hijos de tu amigo del alma, de tu hermana, o de tu nuevo novio son un coñazo, no te lo calles. Que no hay cosa peor que guardarse las cosas dentro de uno. O de una. A los cuatro vientos, ea, odio a tus hijos. Qué carajo.
http://shop.gawker.com/cgi-bin/shopper.cgi?preadd=action&key=GWT08





Por fin, Skype en PSP

Que sí, coñe, que ya era hora. Ya mismo los poseedores del nuevo modelo de PSP (la finita, ya sabéis) podrán usar Skype para llamar a sus amigos usuarios de DS y quemarles la sangre. Ellos a su vez les responderán esgrimiendo las listas de ventas que ven en los foros y tal. Todos contentos.
www.skype.com





De tu parato favorito a la tele

Ya no hace falta ni tener el portátil enchufado a la tele. El PC2TV permite visualizar gráficos, vídeo y demás desde nuestro dispositivo favorito directamente en la tele. Es más, podemos escuchar la música de nuestro ordenador en el HiFi de casa sin cables.
www.oki.com

Pa que te revienten las orejas

Ya seas DJ o diyi, o jugón de esos que les gusta que retumbe el bloque entero mientras echas una partida, o bien quieres que el vecindario entero se aprenda la nueva de María Villalón (?), la caja DMX 6 Fire USB de Terratec es enterita, pa ti. Ya aprenderán a decirte que bajes esa música, ya.
www.terratec.com

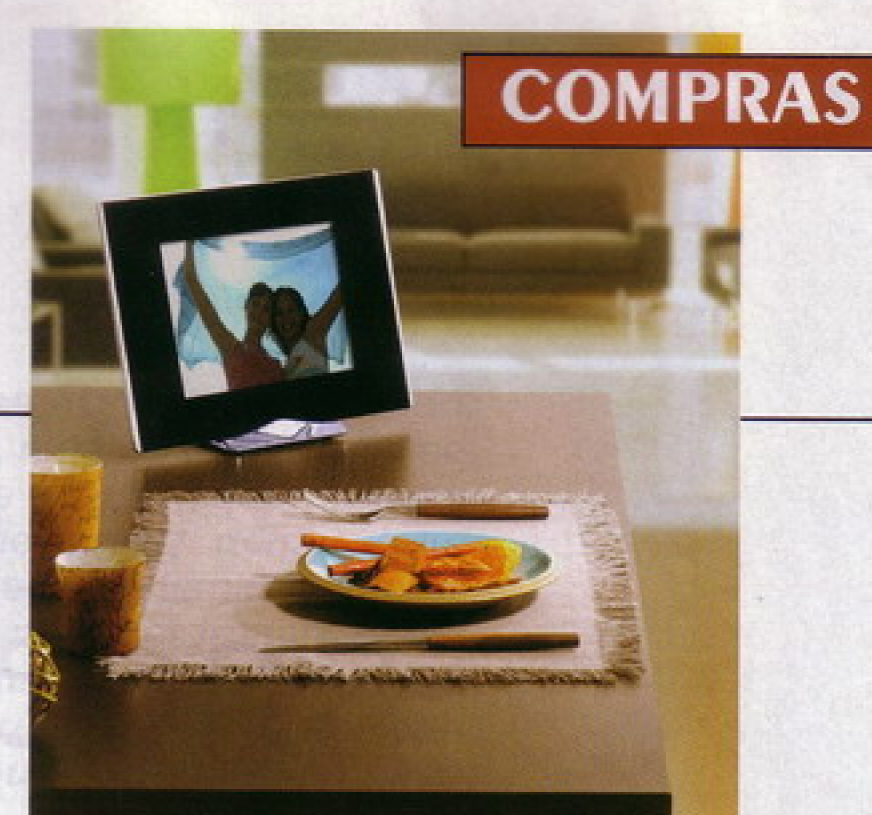






Marco digital para iPod

Estamos en la era del marco digital. Y es que los hay de todos los colores y sabores. Por ejemplo, este incorpora dock para nuestro iPod, en vez de tener que estar tirando de tarjetas o de pendrives USB. Bueno, también podemos usar esos dispositivos, pero ya que nos han regalado el nuevo modelo de iPod, pues...
http://www.engadget.com/2007/12/21/musteks-pf-i700-digiframe-rocks-an-ipod-dock/



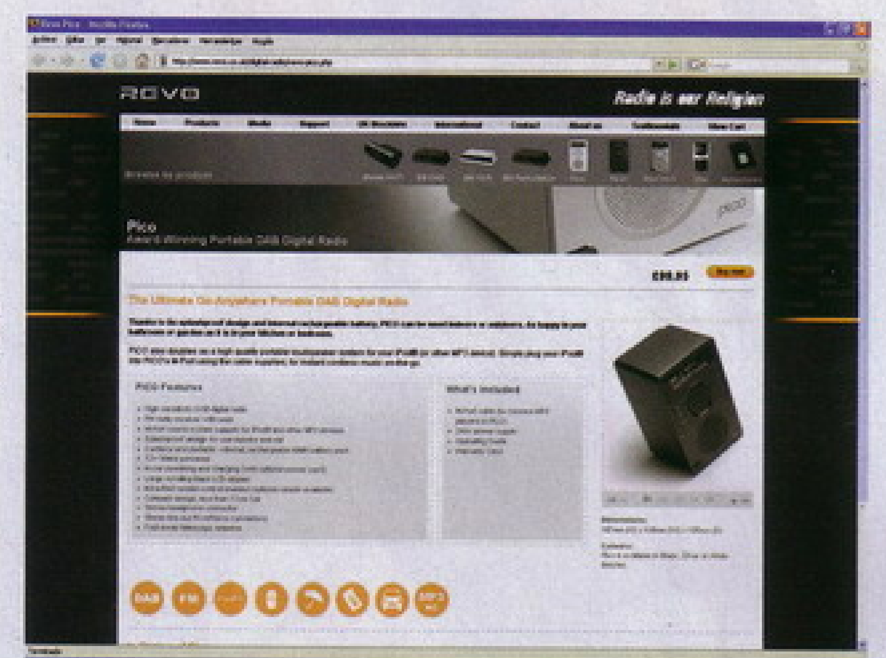
Y más marcos digitales, oiga

Ya lo decimos, esto es una invasión en toda regla. Y llegan modelos de todo tipo. Este permite recibir y transmitir imágenes y demás archivos multimedia sin cables... Eso sí, usando un software propietario. Cuándo aprenderán. Bueno, ahí queda la sugerencia.
http://www.wirelesspixxa.com/



A la rica seta... Luminosa

Que no, que estas setas no se comen, panda de enfermos. Lo que aquí venden son lámparas con forma de setas, bastante parecidas a las de Super Mario por cierto. Un toque gamer para el dormitorio o el salón.
http://usb.brando.com.hk/prod_detail.php?prod_id=00396



El arradio prefesto

El Pico de Revo no es una versión cyberpunk del clásico de Eloy de la Iglesia, sino una pedazo de radio digital portátil, con un montón de posibilidades y funciones, para llevarnos nuestras emisoras favoritas a todos los sitios con mucha más calidad que cualquier tlansitor.
http://www.revo.co.uk/digital-radio/revo-pico.php





El stylus para tu iPhone

Era de esperar, y no será el último stylus que se lance para el iPhone y el iPod Touch. Que en pleno invierno a ver quién es el guapo que se quita los guantes para darle a la pantallita, hombre.
http://www.tenonedesign.com/stylus.php

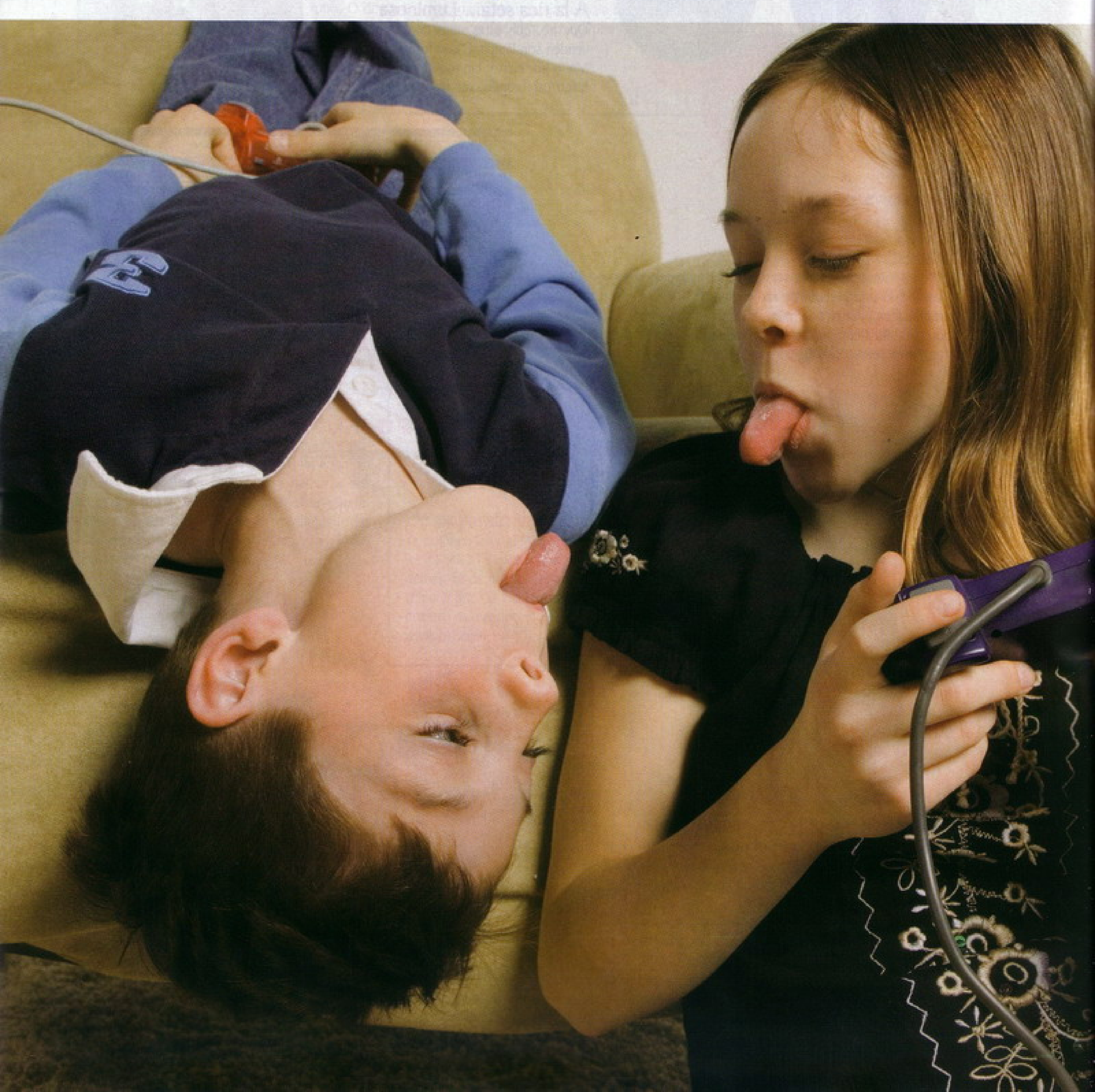


El Eje del Mal queda aquí mismo

Nada como asustar un poco al vecindario (si decimos aterrorizar no iban a tachar de inapropiados... Ups) con unos modestos misiles lanzados con este dispositivo USB. Como lo vea algún paranoico, ya mismo están vetando los dispositivos USB en más de un país, fijo.
http://www.dreamcheeky.com/index.php?pagename=product&pid=41

¡Independencia!

Sácale la lengua a la industria del videojuego (*)



No hace tanto tiempo, antes de las conexiones ADSL y de que todo Cristo tuviera dos o tres consolas en el salón, más de un usuario se paseaba por la Red en busca de otro tipo de videojuegos para su PC. Ya saben, los famosos shareware, freeware y demásware. Queda claro que el panorama ha cambiado, pero las ganas de jugar a todo tipo de juegos sigue estan ahí. Y además del inmarcesible catálogo para PC existe todo un mundo de posibilidades, en el que por un poco de nuestro dinero obtendremos un montón de entretenimiento, y de paso daremos alas a una comunidad que bien se lo merece. Son los juegos independientes.

Pisando fuerte

Los juegos independientes, sencillamente, son esos que no tienen distribuidor oficial, o que no han sido producidos por grandes estudios. Vamos, como en las películas, o esos grupos de música que le gustan tanto a Monmagan. Ojo, no estamos hablando de juegos gratuitos ni nada por el estilo. Estos juegos valen su dinerito, aunque poco, pero hay que pagarlo. Por supuesto, muchos de estos juegos disponen de demos y demás formas gratuitas para probarlos y pagar por sus versiones completas si la cosa nos ha hecho gracia. Como queremos que quede claro que esto no ha sido inspiración nuestra, todo vino por un post del foro de Neogaf (¡sí! Ahora hacemos artículos enteros a partir de posts de foros de Internet. Nos vamos superando, ¿eh?), que hacía referencia a la publicación online de videojuegos 1up. En este post se repasaban los mejores juegos independientes del pasado año, y la verdad es que la mayoría ponen los dientes pero que muy largos. Hay de todos los géneros y la mayoría prometen bastante. El post en cuestión, a partir del cual se puede seguir la pista de las webs oficiales de estos juegos es http://www.neogaf.com/forum/showthread.php?t=220233.

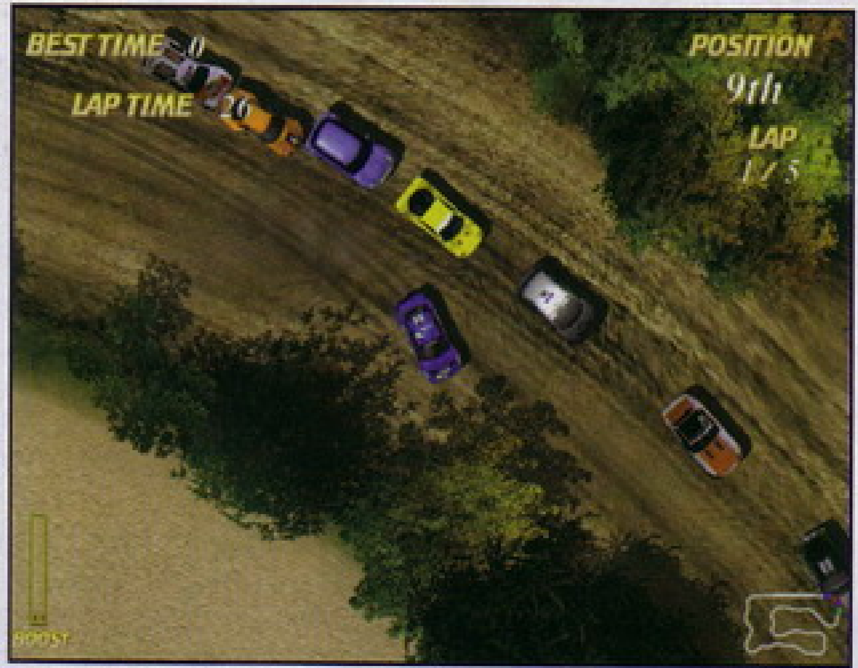
El caso es que quizás nos hemos perdido durante un tiempo entre tanta ROM, tanta ISO y tanta Wii y no le hemos prestado la suficiente atención al mundo de los videojuegos independientes. Y puede que nos hayamos estado perdiendo demasiado. Por eso recurrimos a esta lista, en la que hay juegos como Auto Cross Racing, Peacemaker, Star Defender 4 y Machines at War, en plan llamada de atención. Por todo el mundo (lo cual incluye España) se están creando videojuegos que, por no pertenecer a los entornos a los que se presta más atención (ya sea de la industria o del software libre) no deberían quedarse sin reseña. A ver si a partir de ahora hablamos más de juegos independientes y de sus virtudes. Queda dicho. <

Algunos videojuegos independientes

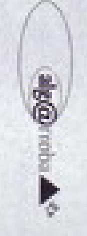
si sois muy vagos para patearos el post citado de NeoGaf, o por azares del destino ya no existe, os adelantamos las direcciones de los juegos independientes que se ganaron el corazón de los aficionados el pasado año.

http://www.regnow.com/softsell/visit...e&vendor=11811
http://www.plimus.com/jsp/redirect.j...rrer=cyrus_zuo
http://studioeres.com/immortal/
http://jng.rakeingrass.com/
http://www.awem.com/star_defender_4/
http://www.peacemakergame.com/
http://www.kjmsoftware.co.uk/auto_cross_racing/auto_cross_racing.htm
http://www.bit-blot.com/aquaria/index.html
http://www.blitwise.com/neonwars.html
http://www.soldak.com/Depths-of-Peril/Overview.html



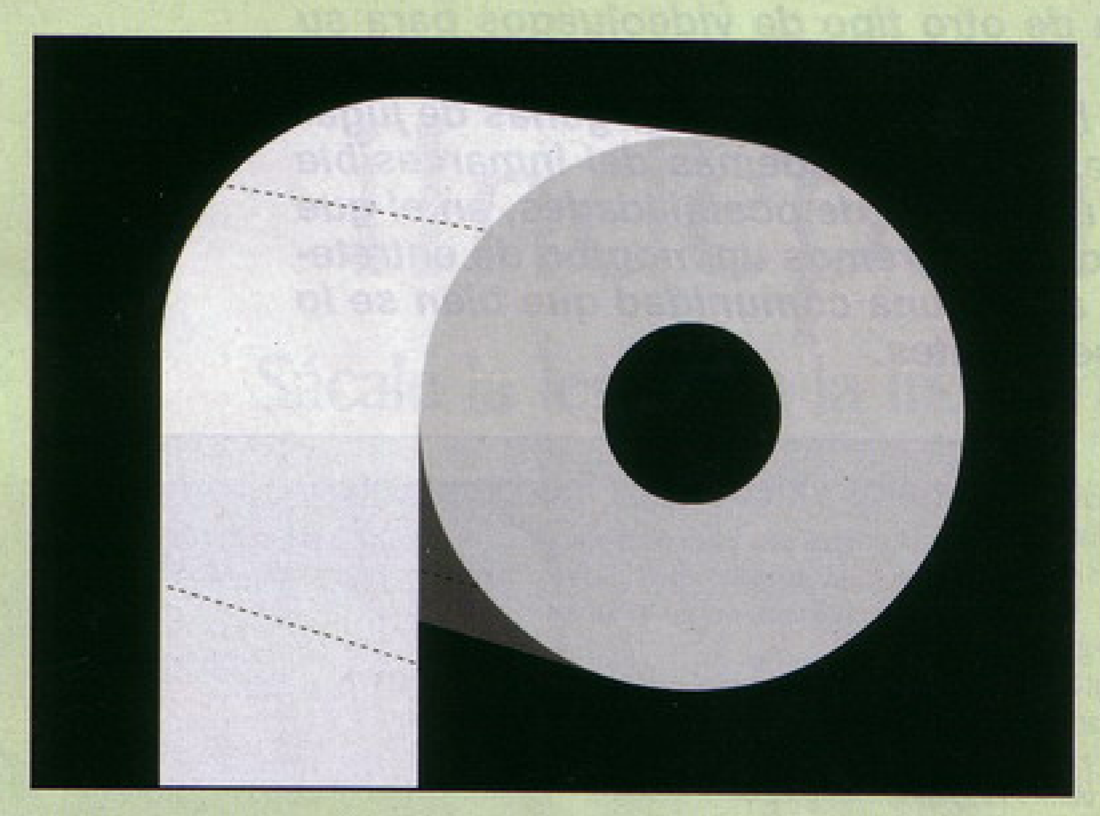


(*) Aunque solo sea un rato, que tampoco vamos a ponernos extremos. Y que queremos que nos sigan enviando jueguecitos esa gente tan simpática de Konami, Sega, Nintendo, EA, Atari, THQ, Proein, Friendware, Vivendi Universal Games, Nintendo, Take2, FX, Sony, Microsoft, Activision y todo aquel que nos hayamos olvidado. Conste en acta, pardiez.



WEB del mes

http://www.papertoilet.com/

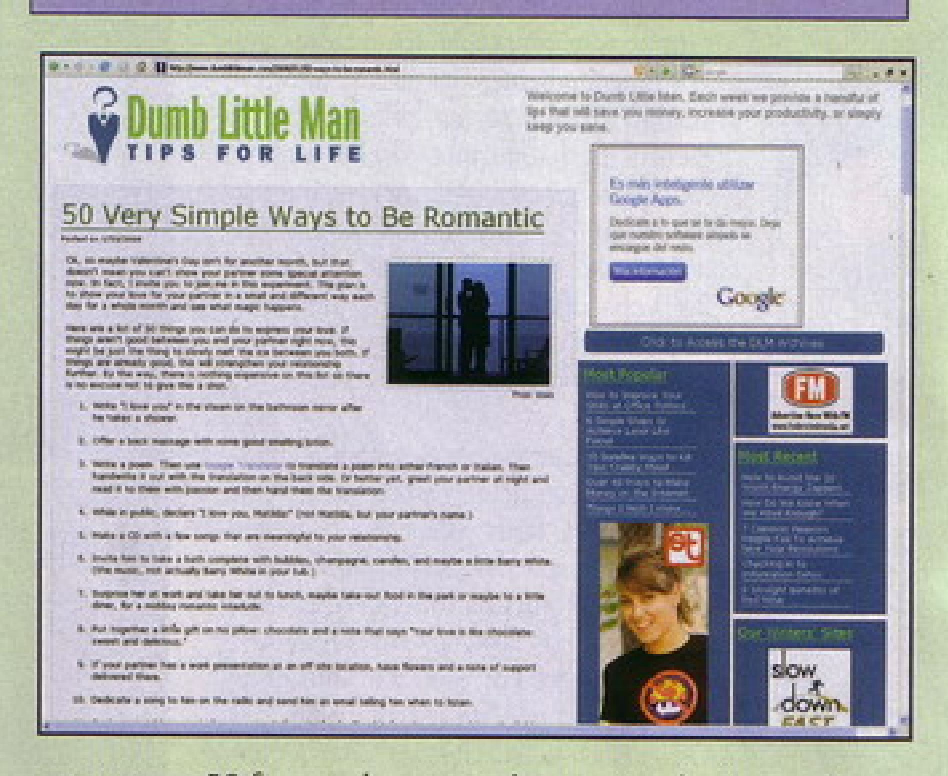


A ver, de entre todas las cosas que usamos a diario, ¿cuál querríamos que fuera eterna e inagotable? Seguro que alguno saldría con una lista bien larga, pero a la hora de la verdad, solo unos pocos artículos se merecen tener la propiedad de ser inagotables. Y uno de ellos es, ineludiblemente, el papel higiénico. Ni los pastelitos, ni los condones, ni los tebeos de Batman. Porque la situación de encontrarse sin papel higiénico es, sencillamente, terrorífica. Más de uno se habrá encontrado en tal tesitura, y la solución, créannos, no es nada fácil. Se han roto amistades inquebrantables y matrimonios inexpugnables por un quítame allá esa cortina mancillada. Pero para que no pierdan la calma, el sosiego ni la fe en la humanidad, estamos ante el primer paso para que no suceda nunca más. Lo de quedarse sin papel, queremos decir. Esta página web ha inventado el papel interminable. Ya, ya, por ahora es todo virtual, pero seguro que dentro de poco evolucionará a una realidad física y tangible y, por lo tanto, utilizable. Que lo de los papeles y las tintas virtuales esas están a la vuelta de la esquina, hombre. Imaginen sacarse la PDA del bolsillo en esos momentos de inquietud y obtener una fuente inagotable de papel higiénico. Que le den el Nobel al que lo haga, leñe.

WEB Chorra

http://www.dumblittleman.com/2008/01/50-ways-to-be-romantic.html

Llega febrero y, una vez más, todos tenemos que dominar las artes del amor, de la seducción y la ternura. Y el resto del año, a escupirse cada vez que nos vemos, ¿no? Hombre, la situación nos ha salido pelín extrema, pero sirve para denunciar eso de que por San Valentín hay que convertirse en el amante perfecto, y todo por un solo día, del cual parece depender el curso de la relación el resto del año. Y no, no son formas, que el cariño hay que cultivarlo todos los días. Pero en fin, como siempre habrá quien gruña los demás días, pero ese en concreto se exprese canturreando letras de Elton John, sacamos esta página web,



que repasa 50 formas de ser romántico cual Glenn Medeiros. Y sí, casi todas son de lo más obvias y manidas, pero nunca se sabe lo faltos de recursos que pueden andar nuestros lectores... Y más de un redactor de @RROBA. De nada, y que haya suerte.

STAFF
"¿Pero por qué me sigues sacando, si yo ya no hago nada?": Carlos Verdier
"Calla, calla, siempre viene bien algún nombre de más cuando llegan las quere... las botellas de vino de publicidad": Gaby Ló
arroba1@megamultimedia.com, ya estáis tardando



FONDOS
Envía AFONDO y su código al 7372
Ej: AFONDO 81171 o llama al 806 464 172
2313 2316 2318 2321 2323
3625 3637 3648 3654 3661
50041 5734 5735 5740 5742
5799 5817 5843 5854 5931
727 728 81861 81907 81909
82129 82207 82209 82211 82214
82233 82237 82236 82240 82241
2335 2337 2348 2350 2352
3662 50007 50012 50023 50034
5746 5749 5764 5765 5768
+18
VIDEO REAL
¡Las escenas mas divertidas y mas calientes!
Envía APELI y su código al 7372. Ej: APELI 62015 o llama al 806 464 172
62016 62018 62025
62013 62020 62026
62011 62007 62034
64322 64303 64522
64314 64342 64523
63110 63106 63120
63102 64289 64466
SONIDOS REALES
Envía SONID y su código al 7372.
Ej: SONID 9370 o llama al 806 464 172
F1 Alonso 9843
Sainz Pasada 9844
Gasol Pelota rompe cristal 9845
Pedrosa acelerando 9846
Bobo solemne 9831
España - España España oe oe oe 9793
Españoles Franco ha muerto 9665
kill bill silvido 9476
Coge el telefono que me da la risa 9746
Orgasmo placentero 9761
RELATOS
Los relatos eróticos mas apasionantes!!
TE EXCITARAS COMO NUNCA!
Envía RELAT al 7372
HENTAI
Los fondos manga y hentai mas sexy!!!
Envía HENTAI al 5099
JUEGOS
Envía AGAME y el código del que quieras al 7372
Ej: AGAME 4460
¡Los juegos mas fuertes!
4465
4460
MOVILES COMPATIBLES:
TOP
GRUPO CODIGO
ampe 70682
pain that I'm 70684
o Bravery 70691
entiras Piadosas 70692
uñeca de trapo 70694
loody Mary 70695
upid Girls 70700
y hips dont lie 70714
Opa yo via ace un corral 70722
.O.V.E. 70726
o quiero verla mas 70732
a mi guerrera 70737
e Voy 70740
Dulce Locura 70742
One 70743
eep 70748
Dani California 70751
Ghosts 70756
Corazon de fuego 70759
Ugly 70760
Pump it 70761
REGGAETON
El baile del... 70328
Asesina 70403
Mueve mami 70404
Hasta cuando 70356
Gasolina 70357
Lo que paso 70386
Eres mi baby 70555
Dale Don Dale 7584
Dile 70308
Don keo 70561
Ella y yo 70559
Luna 70387
Otra noche 70388
Pobre diabla 70389
POLIFONICOS
Envía ROLI y su código al 7372
Ej: ROLI 70543 o llama al 806 464 172
SUPERVENTAS
Push the button 70631
Gold Digger 70630
Window Shopper 70629
Pon De Replay 70627
Belly Dancer 70624
Ass like that 70623
Oh 70622
Stick With You 70621
We be burning 70619
Lets Get Down 70617
Come Clean 70615
Goodies 70611
High 70608
Fly 70603
Dare 70600
Advertising Space 70599
Jesus of suburbia 70597
Beverly Hills 70595
All About Us 70594
Dont Cha 70592
Because of You 70589
Yellow Brick Road 70588
My Humps 70583
Tripping 70579
Dont Lie 70578
Cool 70576
Fix You 70574
Wise Men 70572
Ghetto 70571
The One 70569
I dont care 70557
Madonna - Hung up 70556
Shakira - Dont bother 70553
Anastacia - Pieces of a dream 70552
Juanes - Para tu amor 70550
LATINO
El Profe 70665
Como Cambia la vida 70662
Mi mundo si ti 70660
Besos 70655
Marta, Sebas, ... 70654
Querida enemiga 70652
Vacaciones 70580
Rutinas 70551
Nada fue un error 70516
Te regalo 70514
Amar sin ser amada 70503
No 70502
Nada es para ... 70501
Damelo 70500
Ciudad perdida 70455
Ojos de cielo 70430
A la hora de amar 70410
Mi barrio 70407
La tortura 70362
La camisa negra 70361
Volverte a ver 70313
No entiendo 7963
Sentada aqui en ... 7915
Eres 7913
Obsesion 7818
Se me ocurre amarte 7567
Objection 7500
Nuestra vida 70658
Las Palabritas 70527
Te haria una casita 70518
Oleada 70468
La quinta estación - Perdición 70469
Paulina Rubio - Otro tequila 70470
Seguridad Social - A tontas y... 70463
La musicalite - Brisa 70464
CINE/Tv
Matrix Reloaded 7118
La pantera rosa 7121
Sex in the city 7125
Terminator 7126
X-files 7130
Rocky 7518
El ultimo mohicano 7586
Lord Of The Rings 7600
Superman 7622
Tiburon 7624
Brave Heart 7698
Gladiator 7703
Angeles de Charlie 7866
A-Team 7867
Austin Powers 7868
Batman 7869
Conan El Barbaro 7873
Exorcista 7874
Fame 7875
Flashdance 7876
Friends 7877
Harry Potter 7879
Incredible Hulk 7880
Miami Vice 7881
Top Guns 7882
Armageddon 7900
Beverly Hills Cop 2 7903
CSI 7904
El Padrino 7906
Ghost 7908
La Roca 7909
Love Story 7910
Spiderman 70102
La Fabrica de Chocolate 70558
Kill Bill II - Silvidos 70659
ANIMACIONES
Envía XTREME y su código al 7372 Ej: XTREME 4001
4398 4393 4388 4375
4373 4372 4368 4366
4337 4335 4334 4330
4322 4325 4104 4603
Nos reservamos el derecho de utilizar los datos enviados para posibles operaciones futuras. No obstante disponen de un derecho de acceso, de rectificación y de limitación de datos, en lo que se refiere, ya que somos los únicos destinatarios. Mas contenidos en WWW.MOVILXTREMO.COM

¿Se acuerdan qué juego se comentaba en la página ocho de la MicroHobby número 32? ¿Cómo era la portada de la SuperJuegos número 15? ¿Qué juego resultaba después de teclear el listado de la Amstrad Semanal número 10? ¿Les ha apetecido recordar los precios de juegos de Amiga que se vendían a través de Coconut? No necesitan un DeLorean, nuestro amigo el scanner nos abre sus puertas para revivir un fascinante viaje al pasado.

Arde Alejandría, arde

Lo efímero y a la vez eterno que resulta la literatura digital

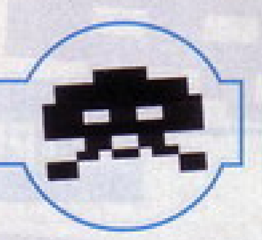
Los scanners lo leen todo

Que caprichoso es el destino, quien nos diría que un aparato de utilidad limitada y de carácter un tanto serio como es un scanner sería tan habitual y prácticamente tan imprescindible en nuestros hogares. No es que sea tan importante como el televisor o la lavadora -y no sé si por ese orden especificamente- pero sí que nos proporciona una calidad de vida, no sé, diferente. Ya no hace falta ir a una copistería para obtener copias de escritos, sean apuntes académicos, sean capítulos enteros de libros o portadas de CD's con su ISBN -International Standard Book Number-, ISSN -International Standard Serial Number- o NIPO -Número Identificación Publicaciones Oficiales-; podemos "fotocopiar" a color, oigan, nos pulimos uno de los sistemas anticopia que antaño y de forma muy simple nos impedían actuar como púberes filibusteros. ¿Alguno recuerda aquella hojita con un millón de



numeros en rojo y azul de la primera aventura gráfica de Indiana Jones? Con la ayuda de un pequeño trozo de plástico rojo transparente se podían descrifar las cifras azules -las rojas quedaban anuladas por la lente del mismo color- e introducir el código que el AtariST o Amiga500 nos pedía al iniciar el juego. Fuera del entorno del entretimiento por video, la publicación Mondo Brutto reeditó sus primeros números en papel de color naranja para cercenar el preocupante tráfico underground de fotocopias. Con un scanner en casa, hecha la ley, hecha la trampa.

Y miren que eso del scanner tiene sus añitos. Vale que allá por la Edad Media cientos de monjes se pasaban su austera vida duplicando y requeteduplicando libracos como si lo de la futura SGAE no fuera con ellos pero no nos iremos tan lejos, tan sólo al 1947, año en el que el señor Russell A. Kirsch experimentaba en la National Bureau of Standards en USAlandia con una supercomputadora de la época, la SEAC -Standards Electronic Automatic



Computer-, y más concretamente con la captación e interpretación de imágenes. El experimento se realizó con una fotografía de su hijo, de tres meses de edad, y el resultado ha pasado a la Historia en forma de imagen de 30.976 pixels -176x176- y en blanco y negro, algo francamente espectacular para ese momento.

¿Sueña la SGAE con scanners mecánicos?

A partir de ahí todo vino rodado, una cosa enlazada con la otra. Pertrechados con scanners en sus casas, no sin algunos haber sufrido los ¿conocidos? scanners de mano, que se llamaban de esta manera por su modo de uso, asiéndolos con la mano y desplazándolos sobre la imagen o documento a reproducir digitalmente, el populacho usa y abusa del scanner. Entrando de puntillas en el terreno que nos interesa, la localización y encuentro de scanneadas sobretodo por vías de material compartido, es como salir a la calle y ver el sol. Con una sencilla búsqueda por internet ustedes pueden encontrar scanneadas de colecciones de cómics completitas, incluso los que acaban de salir al mercado; también pueden encontrar un sindiós de carátulas de CD's y de DVD's, sean de carácter sonoro, visual, audiovisual o videojueguil; y si son cultos y se interesan por la actualidad y la cosa social, publicaciones como Interviu o Playboy también han sido pasto de los scanners. Y no les incito, solamente les informo. Para las féminas y personas homosexuales, publicaciones como Men's Health y GQ también campan a sus anchas. No sigo, que suficientemente escanladizado estoy, no me apetece descubrir cuán lejos puede llegar la perversión humana si encontrara otras como SuperPop, Hola, Lecturas o Qué Me Dices.

En lo vintage, y ahora sí que entramos en tropel al tema en cuestión, las scanneadas serían lo que a un conflicto bélico la guerra fría, un ente semiagazapado, visto por quien quiera verlo, intuido por todos y de función estratégica poco definida. Están ahí, miles de ejemplares scanneados, información vital para cualquier estudioso de la cultura del videojuego, entretenimiento nostálgico para todos. En nuestro país dos son las revistas scanneadas que más bytes de texto han hecho aparecer por nuestras pantallas en forma de comentarios: Micromanía y MicroHobby.







¿QUÉ IMPORTANCIA TIENE QUE UNA NIBBLE MAGAZINE CUESTE 167 EUROS?

SCANdalo, ésto es un SCANdalo

En un intento de resumir el culebrón, tenemos que una persona scanneó ella solita todos los 217 ejemplares de Micro Hobby, que terceras personas se comunicaron con la editorial propietaria, HobbyPress, para rogar una formalización en su libre distribución, que hubo un intento de comercialización a nivel doméstico de los cederrones de las scanneadas con ánimo de lucro y que la editorial denegó, desde entonces, que dichas scanneadas fueran distribuidas por doquier y que por contra se ubicaran en un único reducto, www.microhobby.org. El pitote que se montó en foros y listas de correo daba verdadera vergüenza ajena. Los amantes de lo libre mostrándose comunistas y hostiles, insultos cruzados, amenazas gratuitas, retos públicos... y más aún cuando HobbyPress para celebrar el 20 aniversario de su otra publicación estrella, Micromanía, el marzo de 2005 incluyó en el DVD que acompañaba a ese número 122 las scanneadas de los 35 números que formaron la primera época de la publicación - hasta el día hoy se cuenta tres épocas, siendo la actual la que hace tres.

El rebrote de furia y vomitada del rumor de que esas scanneadas habrían sido expropiadas a scanneadores voluntariosos de fines altruistas se escamparon a diestro y siniestro. La verdad es que de la batalla sólo se conoce la versión de los perdedores, Hobby Press no ha entrado al trapo y no parece que haya razón o motivo para que lo haga, ya que a efectos legales Micromanía es suya y tiene potestad de obrar como crea más conveniente. De hecho en la revista se han ido ofreciendo versiones scanneadas y PDF's de siguientes años y épocas de la publicación, alojados en el DVD con el que se obsequia a los compradores.



Habría que ver y saber que en nuestro país tenemos mucho de lazarillo de Tormes -por lo pícaro- y que a la mínima que se nos da ocasión nos volvemos revoltosillos. Otro personaje scanneó todas las MSX Club, todas las MSX Magazine, todas las Input MSX y todas las MSX Extra y vendió cada recopilación por 30 euros, cuatro cederrones por 120 euracos, todo a expensas de sus editoriales, faltaría más. Como cabría esperar, en la actualidad están todas disponibles aquí y allá en internet, algunas en descarga directa desde algunos sites, otras en constante riego en torrentes y demás animales de carga.

Dimes y diretes

Y es que quien no tiene una suculenta colección de revistas vintage scanneadas es porque no quiere. ¿Qué tal los cien primeros números de Hobby Consolas? ¿Y todas las Loading, GameType, TodoSpectrum o Amstrad Semanal? Ahí fuera, en lo virtual, están todas.

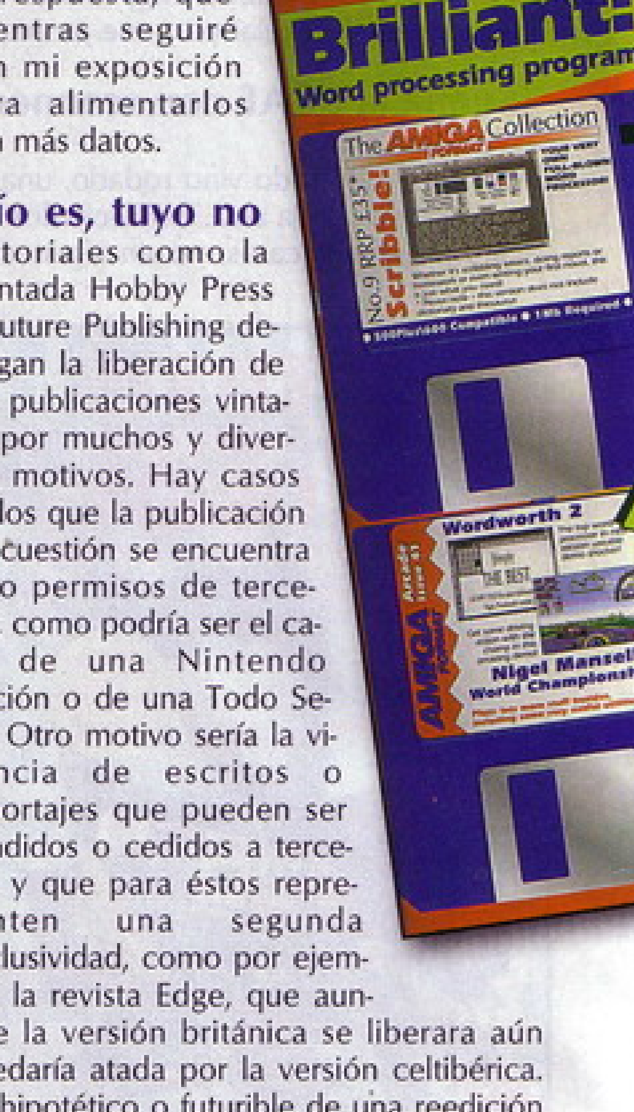
Pasta gansa de la buena. Ahora sí, respondan ¿comprarían, pagarían por revistas scanneadas? Razonen su respuesta, que mientras seguiré con mi exposición para alimentarlos con más datos.

RESPONDAN ¿COMPRARÍAN, PAGARÍAN POR REVISTAS SCANNEADAS?

A nivel internacional la cosa es realmente exagerada. Aunque aún hay numerosas publicaciones que parece inverosímil que nadie las haya empezado a compartir, las disponibles legal o ilegalmente son legión, sean gratuitas o de pago. De las gratuitas, verbigracia de ilegales en su mayoría -con honrosas excepciones como podría ser la Computer Gaming World- poca cosa les puedo contar que no supongan, que alguien con mucho tiempo libre se ha dedicado a scannear revistas y las ofrece en la red de redes para que otra gente con menos tiempo libre se las descargue. Las de pago tienen más chicha, donde van a ir a parar, que le ofrezcan por unos 15 euros toda una colección enterita de ZZap64, por 15 euros más una de Sega Force o por 15 euros más una Atari User versión británica ¿comprarían o no comprarían? No me respondan todavía, háganlo después de leer los párrafos siguientes.

A principios de los 80's apareció en USAlandia la revista Nibble Magazine, dedicada en cuerpo y alma a los Apple II. Su editor y fundador, Mike Harvey, la mantuvo al pie del cañón durante doce años y medio. Como su más absoluto propietario ofrece un lote de scanneadas de los que quitan el hipo: 135 revistas, 27 libros relacionados publicados por la editorial e imágenes en DSK de los programas que aparecieron listados en las revistas. Díganle adiós al hipo: 167 euros.

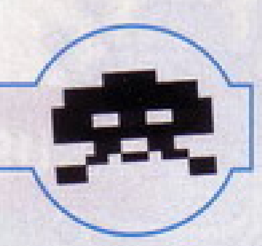
No se confíen, lo que recibirían serían dos DVD's dos con todas las scanneadas en blanco y negro aunque muchas de las revistas fueran publicadas en su día a todo color. Y en una presentación paupérrima, les aviso.



Mío es, tuyo no

Editoriales como la mentada Hobby Press o Future Publishing deniegan la liberación de sus publicaciones vintage por muchos y diversos motivos. Hay casos en los que la publicación en cuestión se encuentra bajo permisos de terceros, como podría ser el caso de una Nintendo Acción o de una Todo Sega. Otro motivo sería la vigencia de escritos o reportajes que pueden ser vendidos o cedidos a terceros y que para éstos representen una segunda exclusividad, como por ejemplo la revista Edge, que aunque la versión británica se liberara aún quedaría atada por la versión celtibérica. Lo hipotético o futurible de una reedición también puede ser causa para no permitir una liberación, ya que los números de épocas anteriores en el caso de Micromanía ha servido de aliciente y revulsivo para que muchos compradores se pasaran por el kiosco a adquirir una revista que habitualmente no compraban. Otra causa menos lógica pero igual de válida es que los contenidos de una publicación sean propiedad de un tercero que ni se sabe por donde anda o que ése mismo no sepa o no quiera saber de permisividades anteriores, por eso no se debe obviar, entre

MUNDOATARI
Nº 9
PUBLICACION PARA USUARIOS DE MICROCOMPUTADORES ATARI





SI HOY PONEN GRATIS LAS REVISTAS DE AYER, ME ESPERO A MAÑANA Y ASÍ TENDRÉ LA DE HOY POR LA PATILLA

otras cosas, que Hobby Press es ahora propiedad del grupo Axel Springer. Future Publiching mantiene esta política, ha adquirido distintos grupos editoriales y no abre concesiones de pasadas o caducas publicaciones porque ésto les supondría una revisión de lecturas y de derechos de los que no les sale a cuenta invertir en su tratamiento burocrático. Un motivo posible más a tener en cuenta: que la publicación se encuentre en curso y definir un punto retroactivo de liberación no quede claro o preste a la confusión, lo que podría traducirse en un descenso de ventas debido al simpático axioma de que si hoy ponen gratis las revistas de ayer, me espero a mañana y así tendré la de hoy por la patilla.

Pero sean de pago o gratuitas, legales o ilegales muchas revistas scanneadas están disponibles, en el caso más inocente podemos encontrar los DVD's de Micromanía en cualquier biblioteca o hemerotéca pública; en los casos menos amables se pueden conseguir mediante descarga digital -algunas revistas son scanneadas y compartidas el mismo día que salen a la venta- o a través de préstamo del DVD físico por parte de algún amiguete. Me da a mí que ustedes son tan buenas personas que si comprasen los DVD's de Nibble Magazine, los de 167 euros que les comentaba antes, no tardarían mucho en prestárselo a sus amigos.

Compra - scannea - vende

Eso del préstamo y del amiguismo también provoca aspavientos. Hace unos meses se inició un ánimo de preservar publicaciones tales como Loading o Hobby Consolas -y digo preservar, supongo que ya me entienden- con un punto lícito y moral en las normas del scanneamiento: sólo recibirían copia de las colecciones aquellos que hubieran colaborado en el proyecto aún con una sola scanneada. El artífice del movimiento declaraba que estas eran sus únicas condiciones, que lo que hicieran luego los colaboradores con las scanneadas ya no era de su competencia, que cabía la muy probable posibilidad de que cualquiera de ellos las compartiera públicamente tan pronto como tuvieran los ejemplares digitales en su poder. ¿Y qué sucedía con los que no podían o no querían colaborar? Existía otra pequeñísima claúsula, que decía que en ese caso uno podía aportar un juego concreto de GameCube a modo de compensación, veintipocos euros, o en su defecto esperarse con la antena puesta a ver si alguno de los colaboradores -que no eran pocos, no- compartía, finalmente, su posesión.

La cuestión es que se montó otro pitote, acusaciones de totalitarismo, blasfemias por lo discrimatorio del asunto, gritos en pro de lo gratis, que la información ha de ser libre y toda la pesca. El caso se cerró abruptamente por motivos personales del scanneador principal, el que ofrecía todas las scanneadas a sus colaboradores, el que sólo pedía a cambio, por defecto, un juego de GameCube, el que arriesgó su puesto de trabajo por utilizar la maquinaria de scanneamiento. Y si me preguntan, sí, uno y sólo uno compró ese juego de GameCube y lo ofreció como trueque. No hace falta que pregunten más.

A las duras o a las maduras el tema de las scanneadas deja indiferente a muy pocos cuando, la verdad, el asunto no tiene ningún sentido. ¿Para qué demonios quiere un vintagenario de a pie tener cien colecciones distintas de revistas en formato electrónico? Se puede comprender que la denostada nostalgia sea la causante de desear tener unos ejemplares que se tuvieron o quisieron tenerse cuando uno era un poco más joven, tener una única colección o unas pocas, las que se vivieron en su momento. De no ser así ¿qué importancia tiene que una Nibble Magazine cueste 167 euros, que una Your Commodore cueste 15 euros o que una Acorn User pueda ser descargada gratuitamente? ¿Qué va a hacer una persona con revistas de Amiga australianas, suecas, italianas y francesas? ¿Qué utilidad tiene poseerlas, o lo que es peor, desearlas? Preguntas que pueden responder -o serles respondidas- si se acercan a www.matranet.net y se toman unos minutos de su preciado tiempo escribiendo a S.T.A.R., su fiel documentalista.

S.T.A.R.<

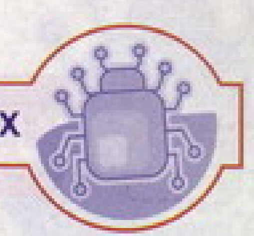




análisis de virus

El método de los Rayos-X

Buenas mis queridos investigadores y fanáticos del hermoso arte de escribir y analizar virus. He encontrado en la red un método bastante interesante que pone en aprietos a los motores de polimorfismo (¡sí!, una vez más).



¿De qué se trata?

El ataque por Rayos-X (RX de ahora adelante), consiste en atacar al cuerpo del virus encriptado por las engines de mutación y polimorfismo.

Cuando un virus infecta, o está en pleno funcionamiento, y éste se trata de un virus polimórfico, su engine polimórfica encriptará el cuerpo del virus, generando uno nuevo.

Generalmente, se utiliza XOR para cifrar el cuerpo del virus. Todo sabemos que XOR es potente siempre y cuando la clave lo sea y respetando ciertas reglas, pero, si utilizamos cadenas pequeñas, o hasta inclusive las generaciones anteriores para cifrar, será fácil de crackear.

No es una técnica nueva, sino, una técnica olvidada, es decir, se utilizaba en los tiempos de DOS, para evitar hacer la emulación del código de los virus encriptados y polimórficos.

Inclusive se le encontró nuevas utilidades para cuando los métodos de Entry Point Obscuring. Ya que también era costoso encontrar esos EP.

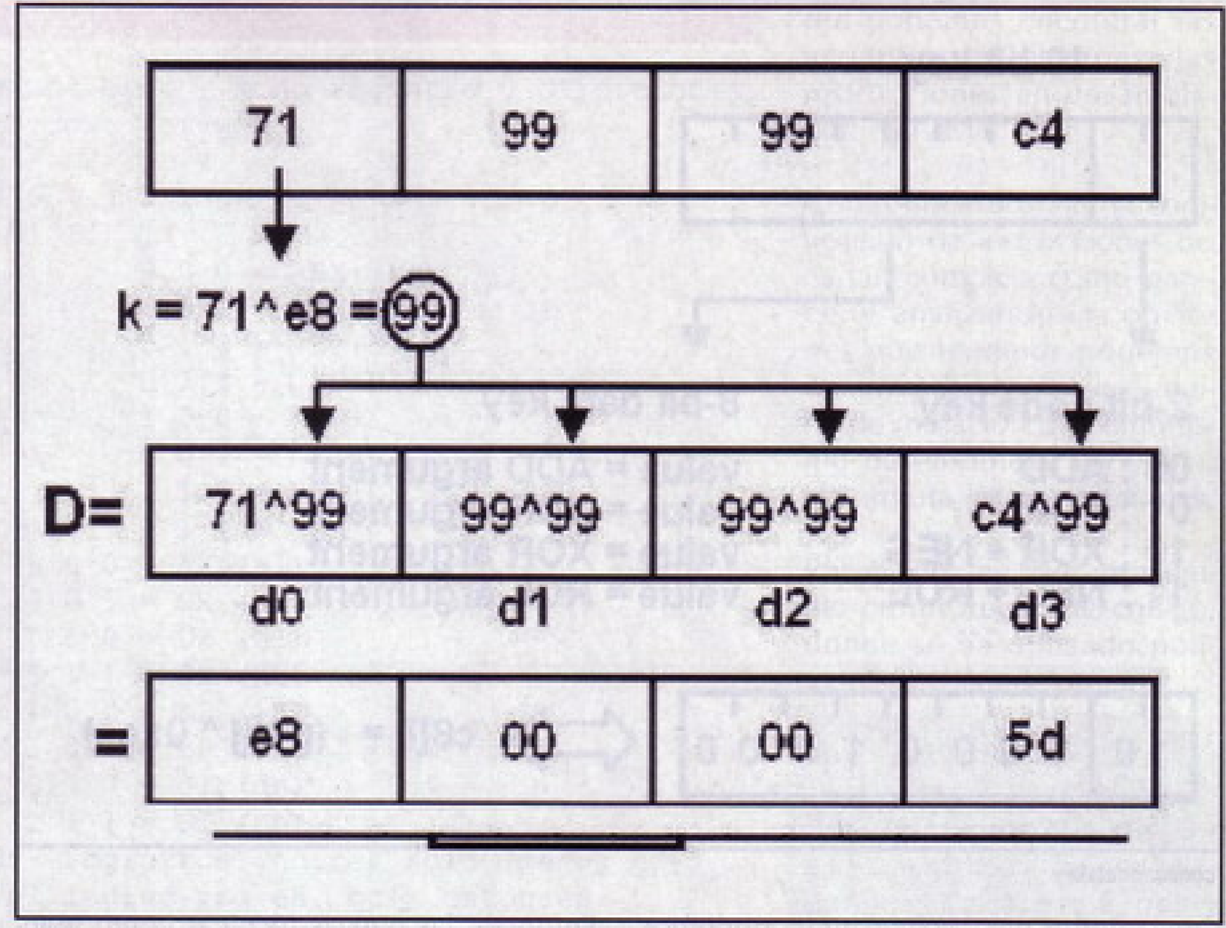
También veremos sus límites como por ejemplo la metamutación y los cifrados en varias capas.

Analogía

Haciendo analogía con la realidad, los RX son utilizados para encontrar algo extraño en el cuerpo humano, o dentro de ciertos lugares donde no se puede acceder.

Los RX son radiaciones electromagnéticas de alta frecuencia.

Buscando en wikipedia, podemos ver esta definición:



basicRX

"Los rayos X es una radiación electromagnética de la misma naturaleza que las ondas de radio, las ondas de microondas, los rayos infrarrojos, la luz visible, los rayos ultravioleta y los rayos gamma.

La diferencia fundamental con los rayos gamma es su origen: los rayos gamma son radiaciones de origen nuclear que se producen por la desexcitación de un nucleón de un nivel excitado a otro de menor energía y en la desintegración de isótopos radiactivos, mientras que los rayos X surgen de fenómenos extranucleares, a nivel de la órbita electrónica, fundamentalmente producidos por desaceleración de electrones. La energía de los rayos X en general se encuentra entre la radiación ultravioleta y los rayos gamma producidos naturalmente.

Los rayos X también pueden ser utilizados para explorar la estructura de la materia cristalina mediante experimentos de difracción de rayos X por ser su longitud de onda similar a la distancia entre los átomos de la red cristalina. La difracción de rayos X es una de las herramientas más útiles en el campo de la cristalografía."

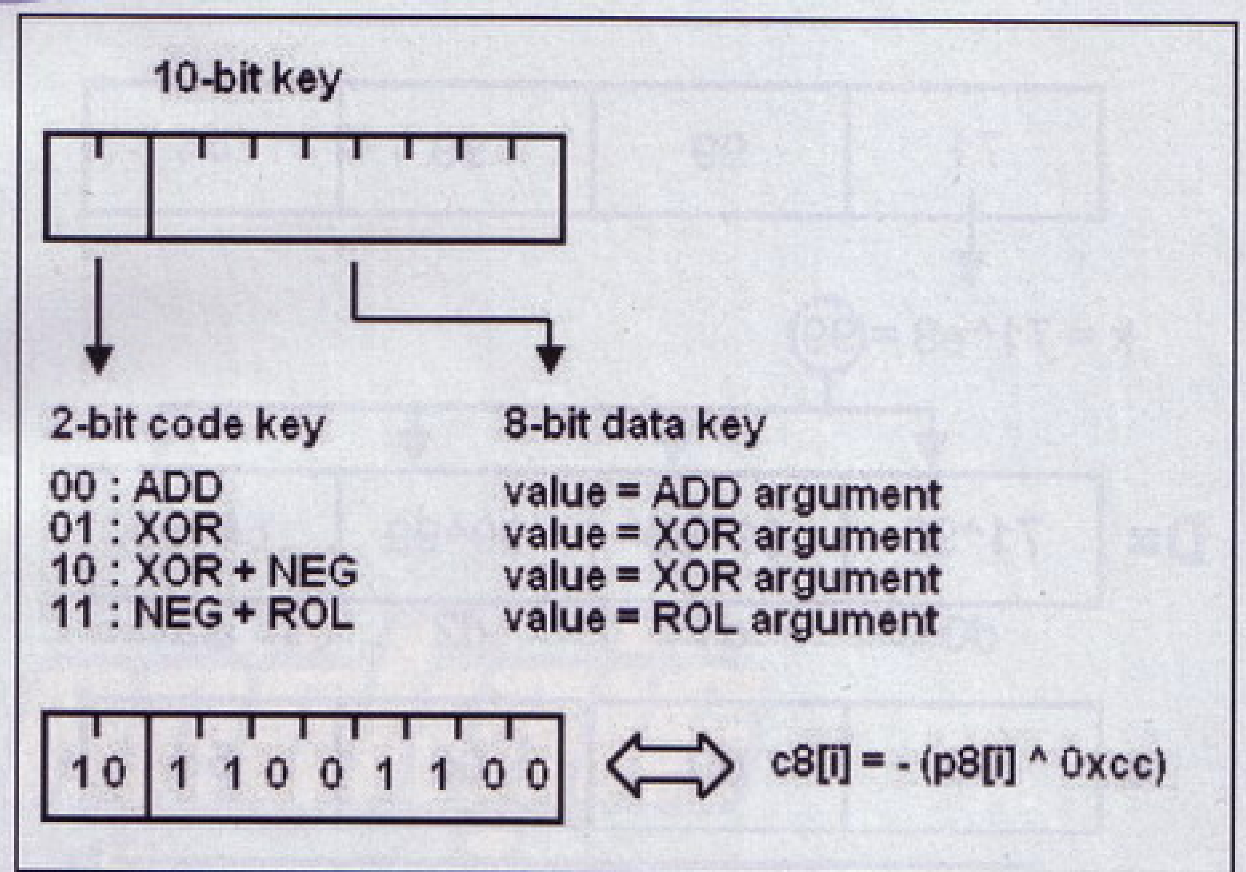
Implementación

Los RX son aplicables sobre el cuerpo del virus, siempre y cuando éste posea una debilidad en su algoritmo de cifrado.

Veremos algunos casos prácticos que Symantec ha utilizado en el pasado, para detectar virus utilizando esta técnica.

Como todos sabemos, la forma más simple (pero no menos compleja) de cifrado es utilizando la operación, XOR, inventado por Verman en los años '30.

Los virus polimórficos, como mencioné antes utilizan XOR con una clave, compuesta por valores entre 0 y 255.



codeanddatakey

Obviamente para volver atrás, podemos probar las claves, hasta encontrar el resultado válido, ya que la clave que suele usarse son bytes repetidos, como por ejemplo: 0x99,0x99,0x99.

La técnica de RX comenzó a ser utilizada en 1991, luego un grupo de investigadores en virus de IBM, patentó ciertas técnicas en la utilización de RX, en el año 1995.

RX fue implementado en diversas engines para diversos antivirus, como por ejemplo F-Prot, soporta RX para encripción mediante ADD y XOR, de a byte, word y dword (8, 16 y 32 bits).

Como dije antes, RX puede ser anulado utilizando diferentes capas de encripción, aunque, como en todo caso, las excepciones valen, el famoso virus W95/Drill.

Kaspersky también tiene implementado el mismo método.

Entonces, las nuevas técnicas como mencioné antes, por ejemplo, EPO, complican y hacen muy costoso el encontrar el loop de desencripción del código, con lo cuál, RX acelera el proceso de ataque sobre el cuerpo del virus.

Inclusive, si algunos virus tienen errores en sus algoritmos de desencripción y/o encripción, que producen al ser emulados loops infinitos o crashes de la aplicación, los RX facilitan el ataque para recuperar el fichero infectado.

RX es readaptado continuamente a los nuevos virus y variantes de los mismos.

El objetivo específico de la técnica de RX es recuperar la clave, dado un grupo de datos cifrados. Lo más importante que se trata de detectar es cuando un virus se encuentra en un objeto, ya sea archivo de texto, imagen, ejecutable, más allá si contiene datos cifrados y cuál es su clave.

Recuperar la clave de un virus cifrado, es solo el primer paso para poder saber si se trata de un virus.

Entonces, luego de recuperar la clave, bloques de datos son desencriptados utilizando la clave y luego comparados contra patrones del cuerpo del virus.

Una gran diferencia entre un ataque a texto plano y RX, es que el ataque a un texto plano cifrado, es a todo un bloque, mientras que RX va en progreso, es decir, se irá escaneando por posiciones, lo que se le denomina RX corrido.

Obviamente debemos saber que cuanto más complicados son los algoritmos de cifrado en los virus, más difícil será aplicar RX.

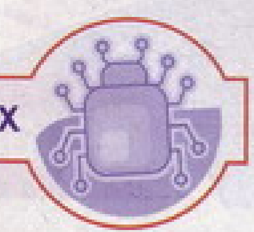
Se trata de uno de los principios más importantes de la criptografía. La seguridad debe estar en la clave y no en el algoritmo en sí.

Ejemplos

Ahora veamos algunos algoritmos de ejemplo, sobre cifrado de un virus. Se han utilizado los dos métodos más conocidos ADD y XOR.

```
                 mov bx,offset
startencrypt
                 mov cx,virus-
length / 2
decrypt_loop:
                 xor word ptr
[ bx] ,12h
                 inc bx
                 inc bx
                 loop
decrypt_loop
startencrypt:
```

Aquí arriba veremos que en BX, tenemos el puntero donde empezaremos a encriptar, y en CX, la cantidad de iteraciones. Fíjense que es la longitud del virus dividido 2 ya que encriptaremos de a word (16 bits).



>>> Listado 1

```
primer byte
     operador
    /   \
 7 6 5 4 3 2 1 0
 0 0 |     0 | |
     |       | 1 = 16 bit
     |       | 0 = 8 bit
     |       1 =  a reg
     |       0 =  a mem
     |
   0 0 0 = add
   0 0 1 = or
   0 1 0 = adc
   0 1 1 = sbb
   1 0 0 = and
   1 0 1 = sub
   1 1 0 = xor
   1 1 1 = cmp
```

```
segundo byte - modo registro y direcciones
modo dest  origen
/ \ /  \  /  \
7 6 5 4 3 2 1 0
|   |     |
|   |     0 0 0 = [ BX+SI+]
|   |     0 0 1 = [ BX+DI+]
|   |     0 1 0 = [ BP+SI+]
|   |     0 1 1 = [ BP+DI+]
|   |     1 0 0 = [ SI+]
|   |     1 0 1 = [ DI+]
|   |     1 1 0 = [ BP+]
|   |     1 1 1 = [ BX+]
|   0 0 0 = AX (al)
|   0 0 1 = CX (cl)
|   0 1 0 = DX (dl)
|   0 1 1 = BX (bl)
|   1 0 0 = SP (ah)
|   1 0 1 = BP (ch)
|   1 1 0 = SI (dh)
|   1 1 1 = DI (bh)
0 0 - registros indices solo (menos bp)
Si el indice reg es [ bp+] entonces
0 0 = [ 1000h] la longitud sera de 16 bit
0 1 - inmediato, es de 8 bits
1 0 - inmediato, es de 16 bits
1 1 registro a registro
    los bits origen, son segundos
    registros usando la misma codificación
    como destino.
```

Luego se va encriptando de a un word por vez, con la clave, que en este caso es 12h. Se incrementa el puntero, dos veces, porque estamos haciendolo de a 16 bits.

```
start:
               mov bx,virus-
length
               mov bp,offset
start
decrypt_loop:
               add byte ptr
[ bp+0Ch] ,33h
               inc bp
               dec bx
               jnz decrypt_loop
```

El registro BX contiene la longitud del código a cifrar, y BP contiene el puntero para saber desde donde se empezará.

En la tercer línea tendremos BP + 0Ch, que se trata de la posición de memoria donde encriptaremos en cada iteración. Es decir, lo que vale BP más una constante definida.

Luego el incremento del registro BP y la posterior decrementación de BX, como contador de iteraciones.

Finalmente el salto que genera el loop, hasta que BX valga cero. Plantearé otros ejemplos de la visión de engines de mutación y polimorfismo. Por ejemplo, en la red podemos encontrar las variantes posibles para las instrucciones en ensamblador: (ver Listado 1)

Como podemos ver, la codificación de instrucciones no es tan compleja como parece, y analizando las opciones que tenemos podemos comprender como una engine de mutación o polimorfismo desensambla, configura, y permuta las instrucciones.

Por último, les daré un ejemplo de un trocito de código, donde se ha utilizado polimorfismo para deformarlo:

```
mov  ax, 808h

Esa instrucción de
allí arriba, podemos
convertirla en algo
como:

mov  ax, 303h        ;
ax = 303h
mov  bx, 101h        ;
bx = 101h
add  ax, bx          ;
ax = 404h
shl  ax, 1           ;
ax = 808h
```

Interesante ¿no?

Conclusión

Bien amigos, aún queda mucho camino por recorrer en las técnicas de RX, en el próximo número seguiremos estudiándolas, analizándolas y enfocándonos más en este análisis interesante. Espero que les haya gustado. Nos vemos en el próximo número.

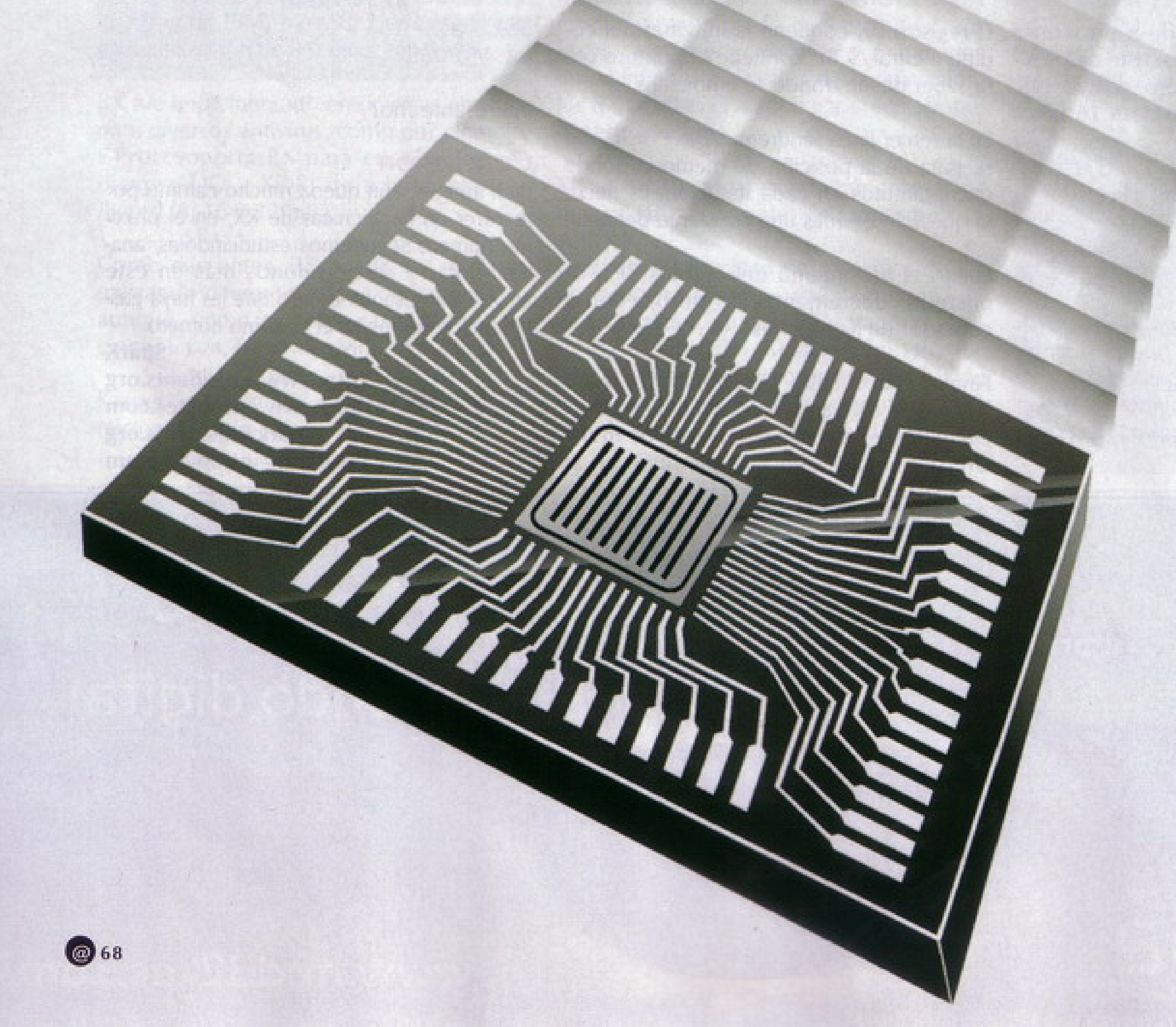
SparK
http://www.disidents.org
http://www.intrabytes.com
spark@disidents.org
arielrm@intrabytes.com

Ya hemos hablado en varias ocasiones de las ventajas e inconvenientes de las diversas filosofías de diseño de una unidad de control. En el caso particular de las unidades de control cableadas, la principal ventaja es su gran velocidad con respecto a, por ejemplo, las microprogramadas; si bien su complejidad es manifiestamente mayor. Una vez que ya conocemos cómo diseñar una unidad de control mediante el método de la tabla de estados, ha llegado el momento de echar un vistazo a otros métodos de diseño alternativos.



Arquitectura de computadores

La unidad de control (V)





Saludos a todos mis apreciados lectores. El mes pasado culminamos el diseño de una unidad de control implementada mediante el método de la tabla de estados. Partiendo del diseño del controlador digital que habíamos realizado con anterioridad, implementamos su circuito y lo unimos a una serie de biestables y puertas lógicas, para lograr obtener el sistema deseado. Tras comprobar su funcionamiento con el test bench pertinente, pudimos dar por finalizado el diseño de dicha unidad de control.

Alternativas de diseño

Por supuesto, el método de la tabla de estados no es el único que podemos seguir a la hora de diseñar una unidad de control. Sí es, en mi opinión, el más sencillo y eficiente para unidades de control cableadas con una complejidad no demasiado elevada, ya que el proceso es muy fácilmente automatizable: en primer lugar, se define una tabla de estados acorde con las necesidades del circuito; a continuación se reduce la tabla a su mínima forma; y por último se implementa mediante biestables y controladores lógicos que pueden ser calculados a partir de dicha tabla.

Pero hay alternativas de diseño cuyo estudio puede resultar muy interesante desde el punto de vista de la electrónica digital. Una de dichas alternativas es el diseño mediante el método de las células de retardo (delay cells), cuya implementación deriva directamente del flujo de ejecución del algoritmo a implementar. Esto significa que la implementación en hardware es total y absolutamente dependiente de la operación que desee realizarse, y de cómo la llevará a cabo el hardware.

Dado que, a nivel de las señales de control emitidas por la unida de control, entre cada dos operaciones es necesario que transcurra un período de tiempo arbitrario, se introducen las denominadas "células de retardo" como el elemento que proporcionará ese lapso de tiempo para que las señales varíen. Además, las señales de control serán afectadas directamente por las entradas y las salidas de dichas células, de forma que esta encadenación de estructuras será la que dicte los pasos a seguir por la unidad de control.

>>> Listado 1

```
ENTITY ffD IS
        PORT (d,clk: IN BIT;
              q,nq: INOUT BIT);
END ffD;

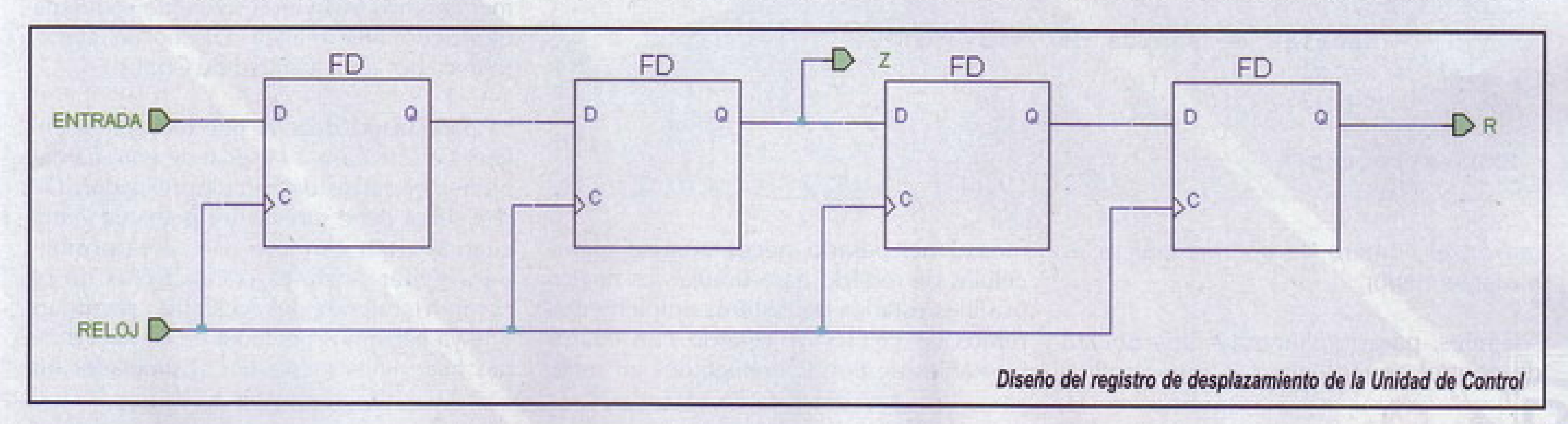
ARCHITECTURE comportamental OF ffD IS
BEGIN
        PROCESS(clk)
        BEGIN
                --Activo por flanco de subida
                IF clk'EVENT AND clk='1' THEN
                        q <= d;
                        nq <= NOT d;
                END IF;
        END PROCESS;
END comportamental;
```

Célula de retardo

Las células de retardo

Dado que el principal cometido de la célula de retardo será el generar intervalos de tiempo regulares en la propagación de una determinada señal, usaremos biestables para obtener el circuito. Así, el diseño de una célula de retardo podría ser el siguiente: (ver imagen Célula de retardo)

Una ventaja que nos proporciona este método frente a, por poner un ejemplo, el método de la tabla de estados; es que el circuito resultante es más sencillo de comprender cuando se observa desde fuera, pues si bien el número de biestables es



Diseño del registro de desplazamiento de la Unidad de Control

>>> Listado 2

```
ENTITY reloj IS
        GENERIC(periodo: TIME:= 60 ns);
        PORT(reloj: OUT BIT:= '1');
END reloj;
ARCHITECTURE comportamental OF reloj IS
BEGIN
        PROCESS
        BEGIN
                WAIT FOR periodo/2;
                reloj <= '0';
                WAIT FOR periodo/2;
                reloj <= '1';
        END PROCESS;
END comportamental;
```

>>> Listado 3

```
ENTITY reg_desp_cr IS
--REGistro de DESPlazamiento para Células de Retardo
        PORT (x,clk: IN BIT;
                z,r: OUT BIT);
END reg_desp_cr;

ARCHITECTURE estructural OF reg_desp_cr IS
--arquitectura estructural del elemento

--declaración de componentes
COMPONENT ffD
        PORT (x,clk: IN BIT;
                q,nq: INOUT BIT);
END COMPONENT;

--declaración de señales
SIGNAL q0,nq0,q1,nq1,q2,nq2,q3,nq3: BIT;

--ubicación de arquitecturas
FOR ALL: ffD USE ENTITY WORK.ffD(comportamental);

BEGIN

        --conexión de la estructura
        n0: ffD PORT MAP(x,clk,q0,nq0);
        n1: ffD PORT MAP(q0,clk,q1,nq1);
        n2: ffD PORT MAP(q1,clk,q2,nq2);
        n2: ffD PORT MAP(q2,clk,q3,nq3);

        --señales de salida del sistema
        z <= q1;
        r <= q3;

END estructural;
```

mayor, el número de puertas lógicas es bastante menor.

Así pues, para implementar una unidad de control equivalente a la que terminamos el mes pasado, necesitaremos cuatro células de retardo para simular los cuatro posibles estados del sistema. Implementaremos las células de retardo con cuatro biestables de tipo D conectados en serie. Por si hay algún despistado por aquí, el código del biestable tipo D es el siguiente: (ver Listado 1)

Uniendo los cuatro biestables, obtendremos un registro de desplazamiento algo particular, que vendrá dado por el siguiente esquema: (ver imagen Diseño del registro de desplazamiento de la Unidad de Control)

Utilizaremos el siguiente reloj para este circuito: (ver Listado 2)

E implementaremos el registro de desplazamiento para las células de retardo de la siguiente forma: (ver Listado 3)

COMO PODRÉIS OBSERVAR SI LO COMPARÁIS CON LA UNIDAD DE CONTROL IMPLEMENTADA EL MES PASADO, EL COMPORTAMIENTO ES EXACTAMENTE EL MISMO

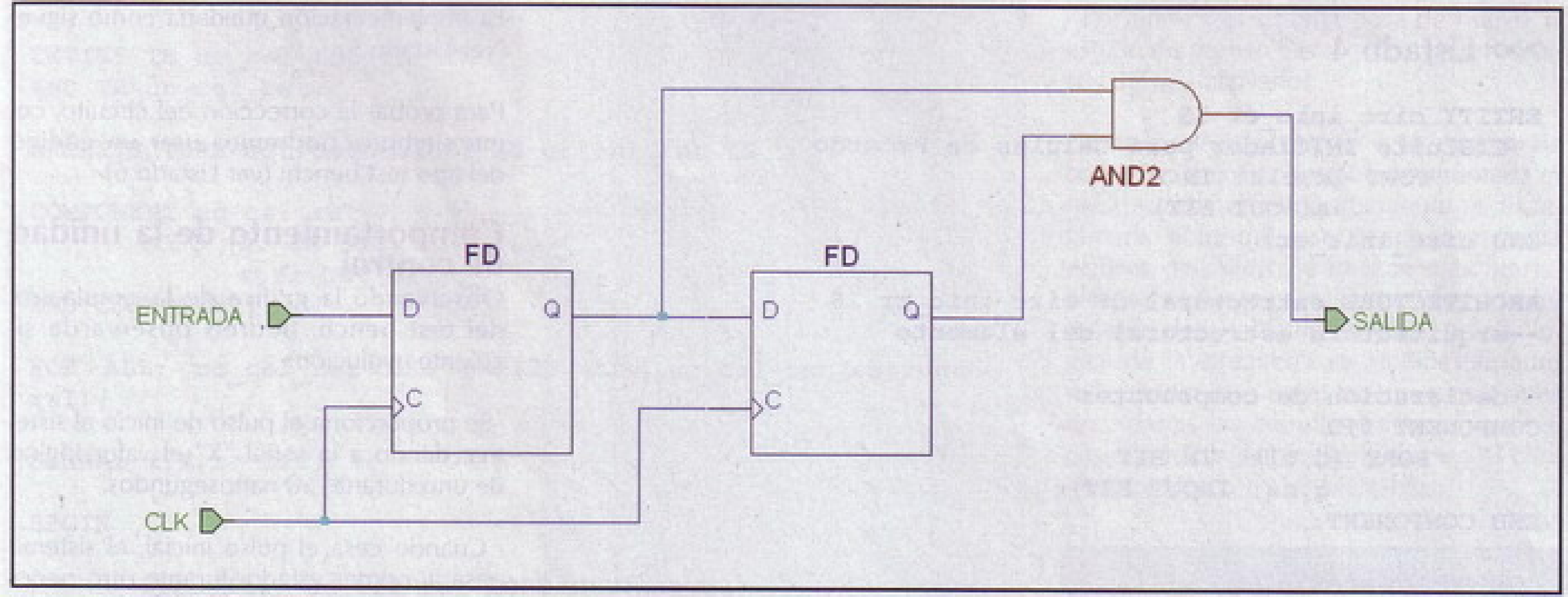
Circuito iniciador

Existe un pequeño problema que suele presentarse a la hora de implementar una unidad de control mediante el método de las células de retardo que aquí ilustramos y, si bien en este caso particular no afecta, suele dar bastantes quebraderos de cabeza si no es tomado en cuenta. El problema consiste en la necesidad de asegurarse que únicamente un biestable en la cadena se encuentra en el estado SET (Q=1), concretamente el primero que debe iniciar la cadena a seguir por el registro de desplazamiento.

Para evitar este problema, se diseña un pequeño circuito encargado de asegurarse de que las señales de entrada del registro de desplazamiento sean las adecuadas. El circuito es muy sencillo, y únicamente necesitaremos dos biestables tipo D y una puerta AND de dos entradas, más una pequeña particularidad que comentaremos tras ver el siguiente esquema de diseño: (ver imagen Diseño del circuito iniciador de la Unidad de Control)

La particularidad de la que hablaba se refiere en este caso a la señal de entrada del primer biestable del circuito iniciador. Dicha señal debe ofrecer un pulso de onda cuadrada tan perfecto como sea posible para evitar posibles oscilaciones en el comportamiento del biestable, recordad que ya hablamos del tema de las oscilaciones hace unos meses. En el simulador no





Diseño del circuito iniciador de la Unidad de Control

supondrá un problema, pues siempre trabajamos bajo condiciones ideales; pero en la vida real obtener una señal cuadrada perfecta no es algo trivial. El cable deberá conectarse a un valor de uno lógico (típicamente cinco voltios como valor Vcc para las familias lógicas TTL), pero interpuesto tendrá que haber un pulsador antirebote. Una pequeña resistencia conectada a la entrada del biestable y a la masa eléctrica protegerá al circuito de posibles sobretensiones.

Una propuesta de implementación del circuito iniciador podría ser la siguiente: (ver Listado 4)

Conectando el sistema

Una vez que hemos diseñado, implementado y comprobado tanto el registro de desplazamiento como el circuito iniciador, simplemente debemos conectar ambos junto al reloj anteriormente mencionado para obtener el circuito secuenciador.

>>> Listado 4

```
ENTITY circ_inic_cr IS
--CIRCuito INICiador para Células de Retardo
       PORT (x,clk: IN BIT;
             s: OUT BIT);
END circ_inic_cr;

ARCHITECTURE estructural OF circ_inic_cr IS
--arquitectura estructural del elemento

--declaración de componentes
COMPONENT ffD
       PORT (d,clk: IN BIT;
             q,nq: INOUT BIT);
END COMPONENT;

COMPONENT and2
       PORT (a,b: IN BIT; z: OUT BIT);
END COMPONENT;

--declaración de señales
SIGNAL q0,nq0,q1,nq1: BIT;

--ubicación de arquitecturas
FOR ALL: ffD USE ENTITY WORK.ffD(comportamental);

BEGIN

       --conexión de la estructura
       n0: ffD PORT MAP(x,clk,q0,nq0);
       n1: ffD PORT MAP(q0,clk,q1,nq1);
       n2: and2 PORT MAP(q0,nq1,s);

END estructural;
```

La implementación quedaría como sigue: (ver Listado 5)

Para probar la corrección del circuito, como siempre, podremos usar un código del tipo test bench: (ver Listado 6)

Comportamiento de la unidad de control

Observando la gráfica de la simulación del test bench, podréis observar la siguiente evolución:

-Se proporciona el pulso de inicio al sistema, dando a la señal "X" el valor lógico de uno durante 60 nanosegundos.

- Cuando cesa el pulso inicial, el sistema pasa al primer estado durante otro período de tiempo de 60 nanosegundos. Podemos observar entonces que "Z=0" y "R=0".

- A continuación, el sistema pasa al segundo estado durante otro período de tiempo de 60 nanosegundos. Podemos observar entonces que "Z=1" y "R=0".

- A continuación, el sistema pasa al tercer estado durante otro período de tiempo de 60 nanosegundos. Podemos observar entonces que "Z=0" y "R=0".

- A continuación, el sistema pasa al cuarto estado durante otro período de tiempo de 60 nanosegundos. Podemos observar entonces que "Z=0" y "R=1".

>>> Listado 5

```
ENTITY uc_cel_ret IS
--Unidad de Control con CÉLulas de RETardo
       PORT (x: IN BIT;
             z,r: OUT BIT);
END uc_cel_ret;

ARCHITECTURE estructural OF uc_cel_ret IS
--arquitectura estructural del elemento

--declaración de componentes
COMPONENT reg_desp_cr
       PORT (x,clk: IN BIT;
             z,r: OUT BIT);
END COMPONENT;

COMPONENT circ_inic_cr
       PORT (x,clk: IN BIT;
             s: OUT BIT);
END COMPONENT;

COMPONENT reloj
       PORT(reloj: OUT BIT:= '1');
END COMPONENT;

--declaración de señales
SIGNAL aux, clk: BIT;

--ubicación de arquitecturas
FOR    ALL:    reg_desp_cr    USE    ENTITY
WORK.reg_desp_cr(estructural);
FOR    ALL:    circ_inic_cr    USE    ENTITY
WORK.circ_inic_cr(estructural);
FOR ALL: reloj USE ENTITY WORK.reloj(compor-
tamental);

BEGIN

       --conexión de la estructura
       rel: reloj PORT MAP(clk);
       ini:        circ_inic_cr          PORT
MAP(x,clk,aux);
       des:        reg_desp_cr           PORT
MAP(aux,clk,z,r);

END estructural;
```



>>> Listado 6

```
ENTITY TB_uc_cel_ret IS
END TB_uc_cel_ret;

ARCHITECTURE estructural OF TB_uc_cel_ret IS

COMPONENT uc_cel_ret
      PORT (x: IN BIT;
            z,r: OUT BIT);
END COMPONENT;

FOR ALL: uc_cel_ret USE ENTITY WORK.uc_cel_ret(estructu-
ral);

SIGNAL x,z,r: BIT;

BEGIN

      circuito: uc_cel_ret PORT MAP(x,z,r);

      PROCESS
      BEGIN

            X<='1';
            WAIT FOR 80 ns;
            X<='0';
            WAIT FOR 80 ns;
            WAIT FOR 300 ns;
            X<='1';
            WAIT FOR 80 ns;
            X<='0';
            WAIT FOR 80 ns;
            WAIT FOR 300 ns;

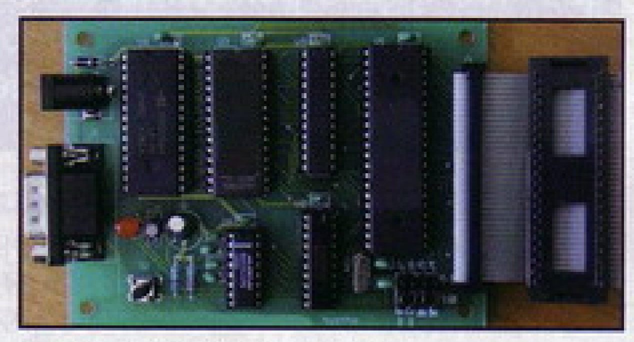
      END PROCESS;

END estructural;
```

Simulación del registro de desplazamiento

- Por último, el sistema pasa de nuevo al estado de reposo hasta que un nuevo pulso vuelva a activarlo.

Como podréis observar si lo comparáis con la unidad de control implementada el mes pasado, el comportamiento es exactamente el mismo, y secuencia las mismas señales de salida. Se utilizan más biestables (seis en este caso, frente a los dos del método de la tabla de estados), pero la lógica de la circuitería es manifiestamente más simple que en el otro sistema, pues recordaréis las complejas funciones lógicas que hubo que implementar en el controlador lógico de los biestables.



Unidad de micro control comercial

El mes que viene...

Este mes hemos podido comprobar cómo es posible, con una implementación radicalmente diferente a la del ejemplo de los dos meses anteriores, obtener un circuito completamente equivalente; el cual presenta sus propias ventajas e inconvenientes en cuanto a rendimiento, coste y complejidad. Sí conviene, no obstante, recordar que aquí estamos realizando ejemplos "de juguete" en comparación con las complejas unidades de control que incorporan hasta los más simples microprocesadores de sistemas empotrados actuales.

El próximo mes tenemos una cita en el mismo sitio, para continuar hablando del interesante mundo de la arquitectura de computadores. Ya sabéis que, como cada mes, tenéis disponible en mi blog el código fuente de cada entrega del curso, para evitar el engorro de copiar el texto de la revista, así como los posibles errores de transcripción. Además, y como siempre, os recuerdo que mi correo electrónico está a disposición de todos vosotros, para cualquier duda o problema relacionado con el curso que deseéis plantear.

Hasta el mes que viene, ¡nos leemos!

Ramiro Cano Gómez
death_master@hpn-sec.net
http://omniumpotentior.wordpress.com<

Parte V

Criptografía asimétrica

Bienvenidos una vez más amigos, hoy tocaremos el tema que nos quedó pendiente en el artículo anterior. La criptografía de curvas elípticas, como funciona este método, que utilidad tiene, sus fortalezas y debilidades.

Introducción

La Criptografía de Curva Elíptica (CCE) se trata de una variante de la criptografía asimétrica basada en curvas elípticas.

La CCE puede ser más rápida y usar claves más cortas que los métodos antiguos (como RSA) al tiempo que proporcionan un nivel de seguridad equivalente.

La utilización de curvas elípticas en criptografía fue propuesta de forma independiente por Neal Koblitz y Victor Miller en 1985.

Los sistemas de criptografía asimétrica se basan en la dificultad de encontrar la solución a ciertos problemas matemáticos.

Uno de estos problemas es el llamado logaritmo discreto.

Encontrar el valor de b dada la ecuación ab = c, cuando a y c son valores conocidos, puede ser un problema de complejidad exponencial para ciertos Grupos finitos de gran tamaño.

¿Qué son las curvas elípticas?

Una curva elíptica es una curva plana, la cuál podemos definir como:

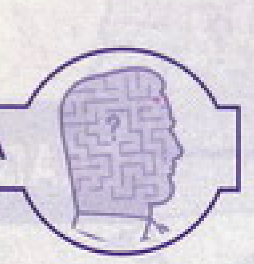
"Curva plana es aquella que reside en un solo plano y puede ser abierta (recta, parábola, hipérbla) o cerrada, (círculo, elipse)."

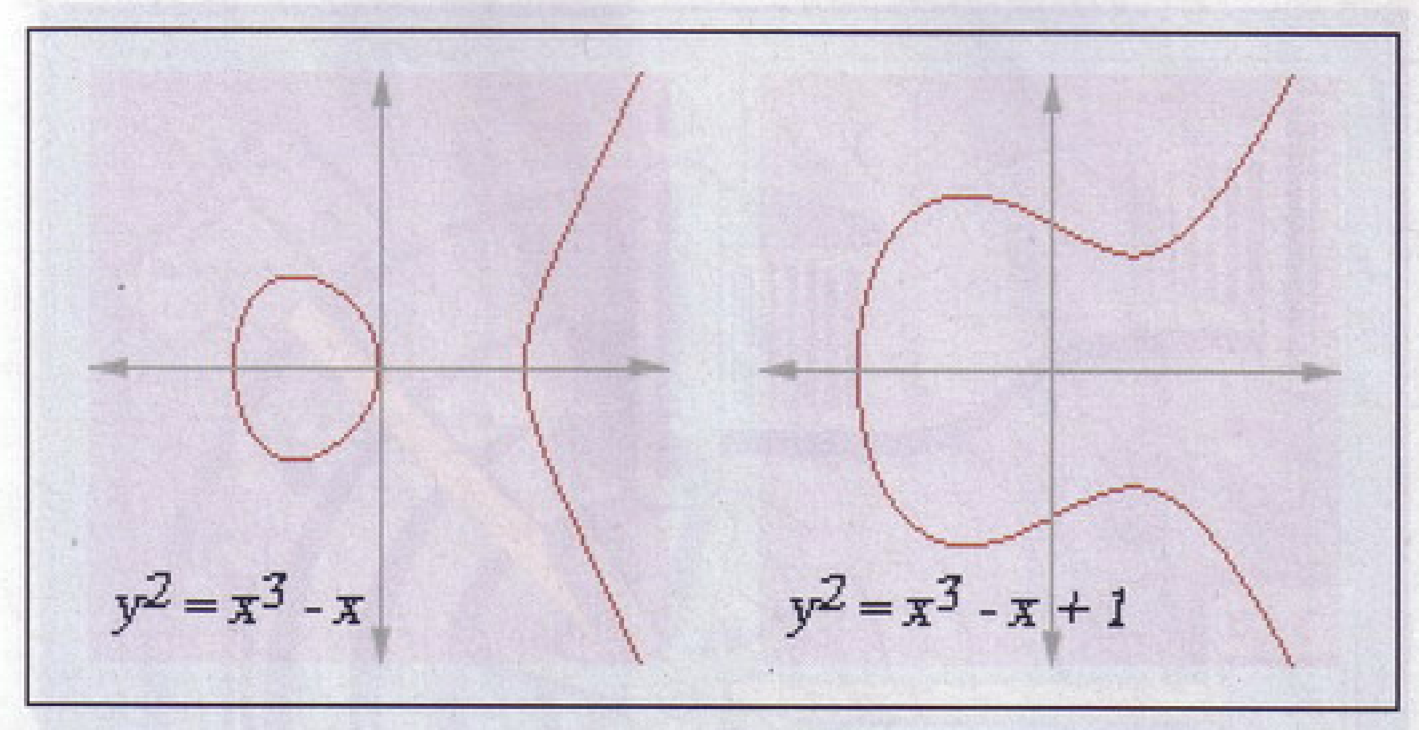
Una curva elíptica tiene la forma:

y2 = x3 + ax + b

Un conjunto de puntos G que forman la curva (i.e., todas las soluciones de la ecuación mas un punto O, llamado punto en el infinito) más una operación aditiva +, se forma un grupo abeliano.

Nº dígitos	Sistema criptográfico	Nº operaciones (cifrado/descifrado)	Nº operaciones (ruptura clave)	Tiempo (ruptura clave con ordena. de 10^9 FLOPS)
30	*RSA* Curvas elípticas	9.0 E 02 2.7 E 04	2.7 E 07 1.0 E 15	0.3 segundos 11 días
35	*RSA* Curvas elípticas	1.2 E 03 4.2 E 04	1.4 E 08 3.0 E 17	1.2 segundos 9.1 días
40	*RSA* Curvas elípticas	1.6 E 03 6.4 E 04	7.3 E 08 1.0 E 20	6.0 segundos 3.0 E 03 años
50	*RSA* Curvas elípticas	2.5 E 03 1.2 E 05	1.4 E 10 1.0 E 25	2.0 minutos 3.0 E 06 años
85	*RSA* Curvas elípticas	7.2 E 03 6.1 E 05	9.0 E 13 3.0 E 42	1 día ---
100	*RSA* Curvas elípticas	1.0 E 04 1.0 E 05	2.3 E 15 1.0 E 50	28 días ---
200	*RSA* Curvas elípticas	4.0 E 04 8.0 E 05	1.2 E 23 1.0 E 100	3.8 E 6 años ---





Si las coordenadas x e y se escogen desde un campo finito, entonces estamos en presencia de un grupo abeliano finito.

El problema del logaritmo discreto sobre este conjunto de puntos (PLDCE) se cree que es más difícil de resolver que el correspondiente a los campos finitos (PLD).

De esta manera, las longitudes dê claves en criptografía de curva elíptica pueden ser más cortas con un nivel de seguridad comparable.

Implementación teórica

En el uso criptográfico, se elige un punto base G específico y publicado para utilizar con la curva E(q).

Se elige un número entero aleatorio k como clave privada, por lo tanto, el valor P = k*G se da a conocer como clave pública.

Si Bob y Alicia tienen las claves privadas kA y kB, y las claves públicas PA y PB, entonces Alicia podría calcular kA*PB = (kA*kB)*G; y Bob puede obtener el mismo valor dado que kB*PA = (kB*kA)*G.

Esto permite establecer un valor "secreto" que tanto Alicia como Bob pueden calcular fácilmente, pero que es muy complicado de derivar para una tercera persona.

Además, Pedro no consigue averiguar nada nuevo sobre kA durante ésta transacción, de forma que la clave de María sigue siendo privada.

Los métodos que son utilizados en la práctica para cifrar mensajes basándose en este valor secreto, consisten en adaptaciones de antiguos criptosistemas de logaritmos discretos originalmente diseñados para ser usados en otros grupos. Entre ellos podemos mencionar a Diffie-Hellman, ElGamal y DSA.

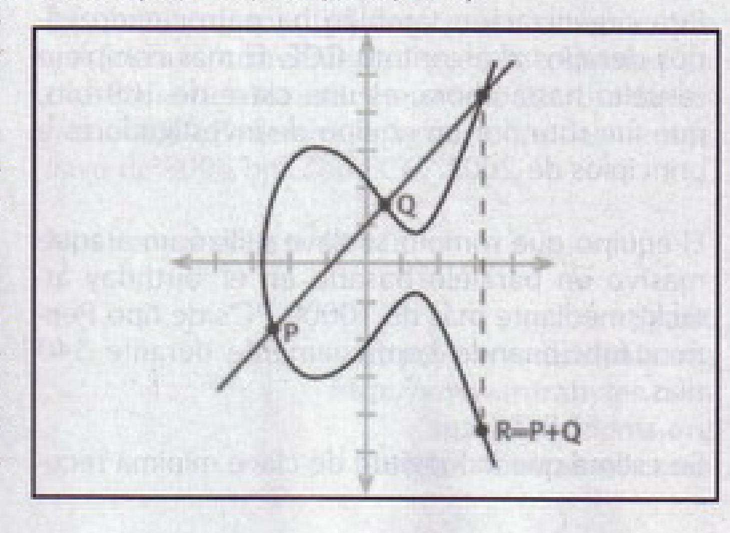
La realización de las operaciones necesarias para ejecutar este sistema es más lenta que para un sistema de factorización o de logaritmo discreto módulo entero del mismo tamaño.

Una característica a davor es que se puede obtener la misma seguridad que RSA u otros algoritmos, mediante longitudes de clave mucho más cortas utilizando CCE, y que, además, puede resultar más rápido que RSA.

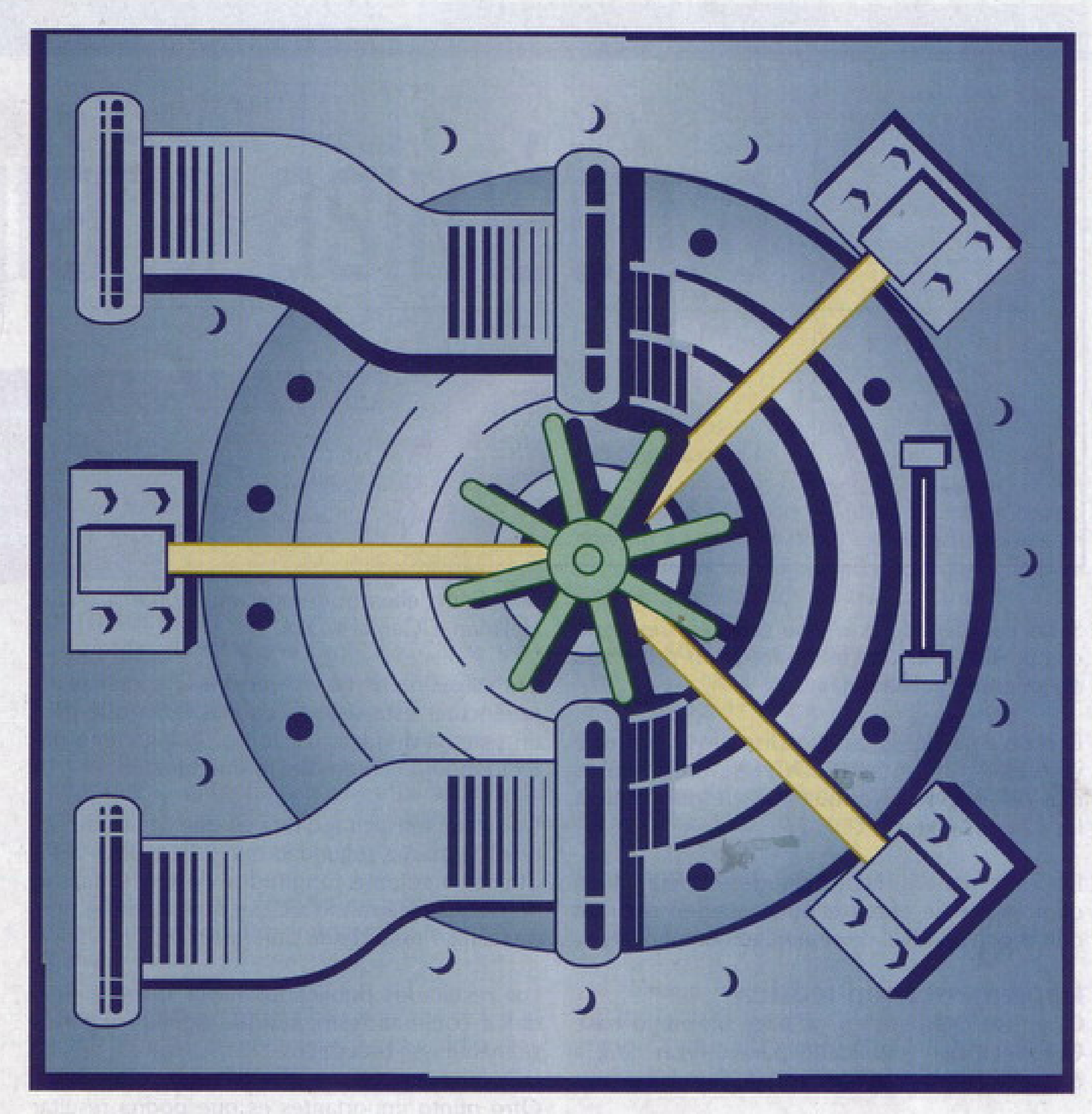
Los resultados publicados hasta la fecha tienden a confirmar esto, aunque algunos expertos se mantienen escépticos.

Otro punto importantes es que podría resultar útil sobre enlaces que tengan requisitos muy limitados de ancho de banda, al poder generar claves poderosas en menor longitud.

NIST y ANSI X9 han establecido unos requisitos mínimos de tamaño de clave de 1024 bits para RSA y DSA y de 160 bits para ECC, correspondientes a un bloque simétrico de clave de 80 bits. NIST ha publicado una lista de curvas elípticas recomendadas de 5 tamaños distintos de claves (80, 112, 128, 192, 256).



CERTICOM ES LA PRINCIPAL EMPRESA COMERCIAL DE CCE, ESTA ORGANIZACIÓN POSEE 130 PATENTES, Y HA OTORGADO LICENCIAS SOBRE TECNOLOGÍA A LA NATIONAL SECURITY AGENCY (NSA) POR 25 MILLONES DE DÓLARES



En general, la CCE sobre un grupo binario requiere una clave asimétrica del doble de tamaño que el correspondiente a una clave simétrica.

Certicom es la principal empresa comercial de CCE, esta organización posee 130 patentes, y ha otorgado licencias sobre tecnología a la National Security Agency (NSA) por 25 millones de dólares.

Esta organización también ha patrocinado varios desafíos al algoritmo CCE. El más complejo resuelto hasta ahora, es una clave de 109 bits, que fue roto por un equipo de investigadores a principios de 2003.

El equipo que rompió la clave utilizó un ataque masivo en paralelo basado en el 'birthday attack', mediante más de 10000 PC's de tipo Pentium funcionando continuamente durante 540 días.

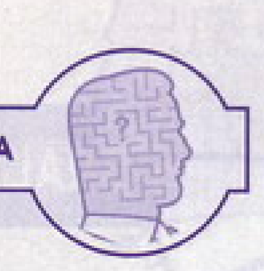
Se estima que la longitud de clave mínima recomendada para CCE (163 bits) requeriría 108 veces los recursos utilizados para resolver el problema con 109 bits.

Las curvas elípticas tienen ciertas características que las hacen especiales en el mundo de la criptografía. Una de estas características consiste en la posibilidad de poder generar un punto en una curva partiendo de dos puntos dados (o incluso de uno). Este concepto es muy fácil de entender partiendo de la figura siguiente.

EL ALGORITMO DE FIRMA DIGITAL PARA CURVAS ELÍPTICAS ESTÁ BASADO EN EL ESTANDAR DE FIRMA DIGITAL DSA. ESTE ALGORITMO OFRECE UN ESQUEMA QUE PERMITE FIRMAR DOCUMENTOS Y VERIFICAR LAS FIRMAS

Algoritmo de firma digital (ECDSA)

El algoritmo de firma digital para curvas elípticas está basado en el estandar de firma digital DSA. Este algoritmo ofrece un esquema que permite firmar documentos y verificar las firmas.Los pasos a seguir para generar claves, firmar y verificar la firma, se muestran a continuación.Alice genera un par de claves:1. Alice elige una curva E con orden #E=fr, de manera que r sea un primo grande.2. Alice busca un punto en la curva de orden r.3. Alice elige



un número aleatorio d situado en el intervalor [2, r-2] y calcula Q=dP.4. La clave pública corresponde a (E,P,r,Q) y la clave privada a d.Alice firma un documento M.(h(M) corresponde al hash de M)1. Alice elige un número aleatorio k en el intervalo [2, r-2].2. Se calcula el punto (x, y)=kP3. R=x mod r4. s=k^{-1} (h(M) +Rd) mod r, si s es igual cero, empezamos de nuevo.5. La firma de Alice es (R,s) y se transmite junto con el mensaje M.Bob verifica la firma de Alice.1. Bob obtiene la clave pública de Alice.2. Entonces w = s^{-1} mod r3. A lo que u1 = h(M) w mod r4. Por lo tanto, u2 = Rw mod r5. (x, y) = u1P + u2P6. Finalmente v = x mod r7. Si v es igual a R, la firma es válida.

OpenSSL: Un ejemplo práctico de firma digital mediante curvas elípticas

Desde la versión 0.9.8 la herramienta OpenSSL ofrece algunas opciones para trabajar con curvas elípticas. No están muy documentadas, pero nos servirán para realizar una pequeña demostración del uso de la firma digital.Para generar un clave ejecutaremos el siguiente comando:

```
$ openssl ecparam -genkey -name
secp224r1 -out key.pem
```

Ahora tanto la clave pública como la privada se encuentran dentro de key.pem.

Podemos extraer la pública con el comando:

```
$ openssl ec -in key.pem -text -
pubout -out pubkey.pem
```

Ya disponemos de una clave con la que hacer pruebas, por lo que generaremos un mensaje que firmar:

```
$ echo "El mensaje de prueba de
h4ck1t!" > msg.txt
```

Y lo firmaremos, operación que solo puede realizar el propietario de la clave privada:

```
$  openssl dgst -sign key.pem -
ecdsa-with-SHA1 < msg.txt >
msg.sig
```

Firmado el mensaje, todo usuario que disponga de la clave pública podrá verificar su procedencia:

```
$ openssl dgst -verify pubkey.pem
-ecdsa-with-SHA1 -signature
msg.sig < msg.txt

Verified OK
```

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, se\ P \neq Q \\ \dfrac{3x_1^{\ 2} + a_4}{2y_1}, se\ P = Q \end{cases}$$

¿Posibles creaciones?

La creación de un protocolo con criptografía de curvas elípticas requiere fundamentalmente una alta seguridad y una buena implementación.

Para el primer punto se requiere que la elección de la curva sea adecuada, principalmente que sea no-supersingular y que el orden del grupo de puntos racionales tenga un factor primo de al menos 163 bits, además de que este orden no divida al orden de un número adecuado de extensiones del campo finito, para que no pueda ser sumergido en él.

Si el campo es ZP, se pide que la curva no sea anómala o sea que no tenga p puntos racionales. Todo esto con el fin de evitar los ataques conocidos.

Para el caso de la implementación hay que contar con buenos programas que realicen la parte aritmética del campo finito, también de buenos algoritmos que sumen puntos racionales, tanto en el caso de Zp como F2n, en este último se toma una base polinomial que tenga el mínimo de términos.

Por ejemplo un trinomio para generar los elementos del campo finito, esto si la implementación es en software, y se toma una base normal si es en hardware. Además de contemplar que las operaciones de puntos racionales pueden hacerse en el espacio proyectivo, esto elimina el hacer divisiones, ahorrando bastante tiempo.

Conclusión

Bien amigos, hemos visto la criptografía asimétrica utilizando curvas elípticas. Es un método bastante curioso, útil y creo personalmente que por demás conveniente, porque estamos en presencia de una manera más poderosa de cifrar datos. ¿Podemos imaginar el poder de una llave de 8096 bits con ECC? :)

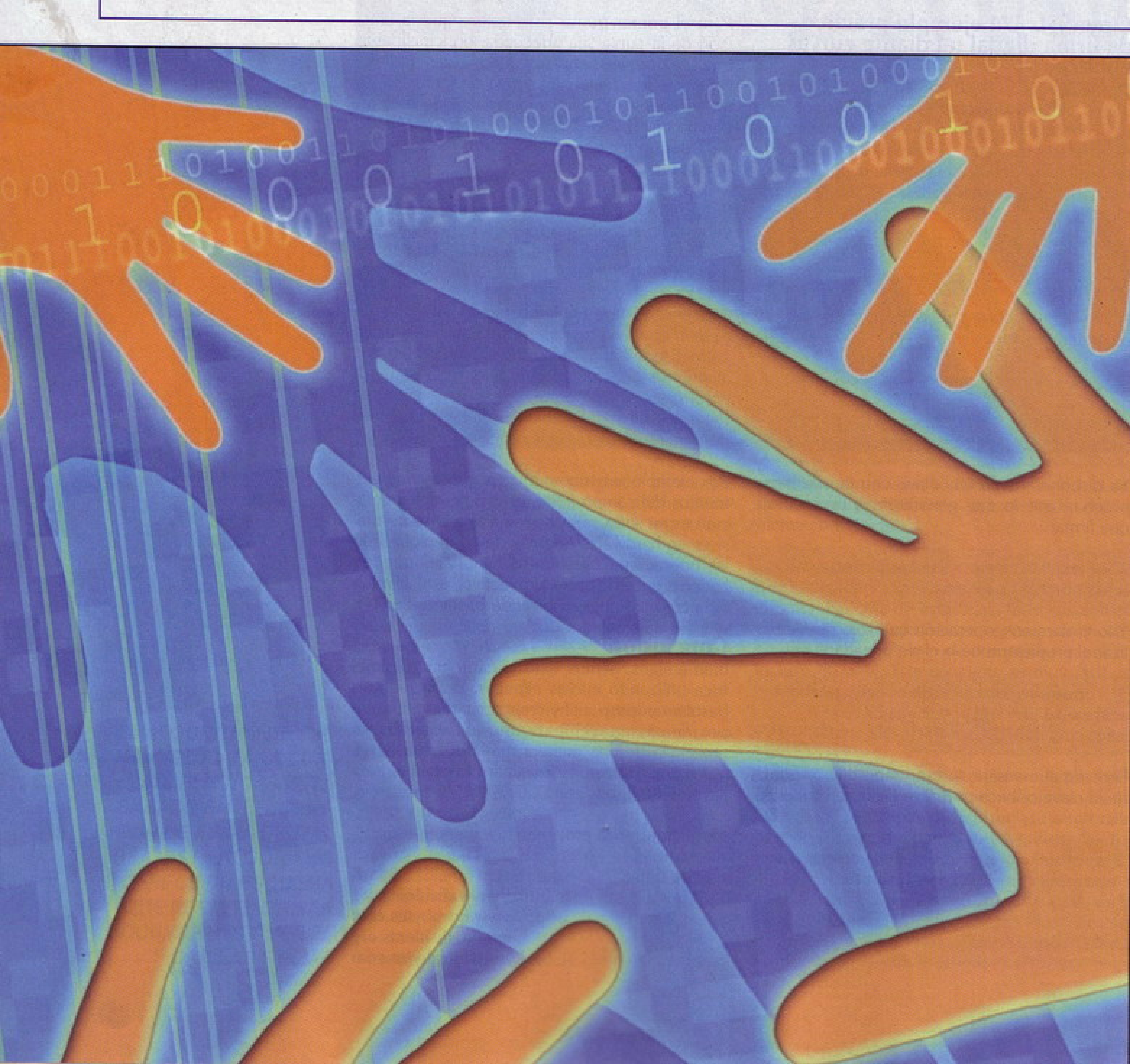
Nos vemos en la próxima.

SparK
http://www.disidents.org
http://www.intrabytes.com
spark@disidents.org
arielrm@intrabytes.com

Criptografía clásica

Cifradores por sustitución poligrámica

Hasta el momento todos los cifradores que hemos visto cifran un carácter del texto en claro con uno del alfabeto o alfabetos de cifrado, salvo el cifrador por homófonos.





Ahora veremos un sistema utilizado por el Reino Unido en la Segunda Guerra Mundial. Este sistema, a diferencia del resto transforma poligramas, es decir, conjuntos de dos o más caracteres para transformarlos en un conjunto de igual número de caracteres pero cifrados con unas reglas concretas.

Introducción

Este sistema consistía en separar el texto en claro en una matriz de 5x5 en la cual se encontraban representadas 25 letras, de las 26 del alfabeto inglés.

Para una mayor seguridad, se incluía una clave al principio, omitiendo los caracteres repetidos y rellenando finalmente con el resto de caracteres del alfabeto.

A	B	C	D	E
F	G	H	I/J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

En el caso de incluir una clave, por ejemplo "CLAVE" la matriz quedaría del siguiente modo:

C	L	A	V	E
B	D	F	G	H
I/J	K	M	N	O
P	Q	R	S	T
U	W	X	Y	Z

Este sistema cifra los caracteres del mensaje en claro M(1)M(2) como C(1)C(2) siguiendo las siguientes reglas:

1 - Si M(1) y M(2) se encuentran en la misma fila, C(1) y C(2) serán los caracteres que se encuentren a la derecha de M(1) y M(2) respectivamente, por lo tanto, algunas cifras serian del siguiente modo:

LA - AV
CA - LV
LE - AC

2 - Si M(1) y M(2) se encuentran en la misma columna, C(1) y C(2) serán los caracteres inminentemente debajo de ellos respectivamente, de forma similar a la regla 1. Ejemplo:

LQ - DW
CI - BP
VS - GY

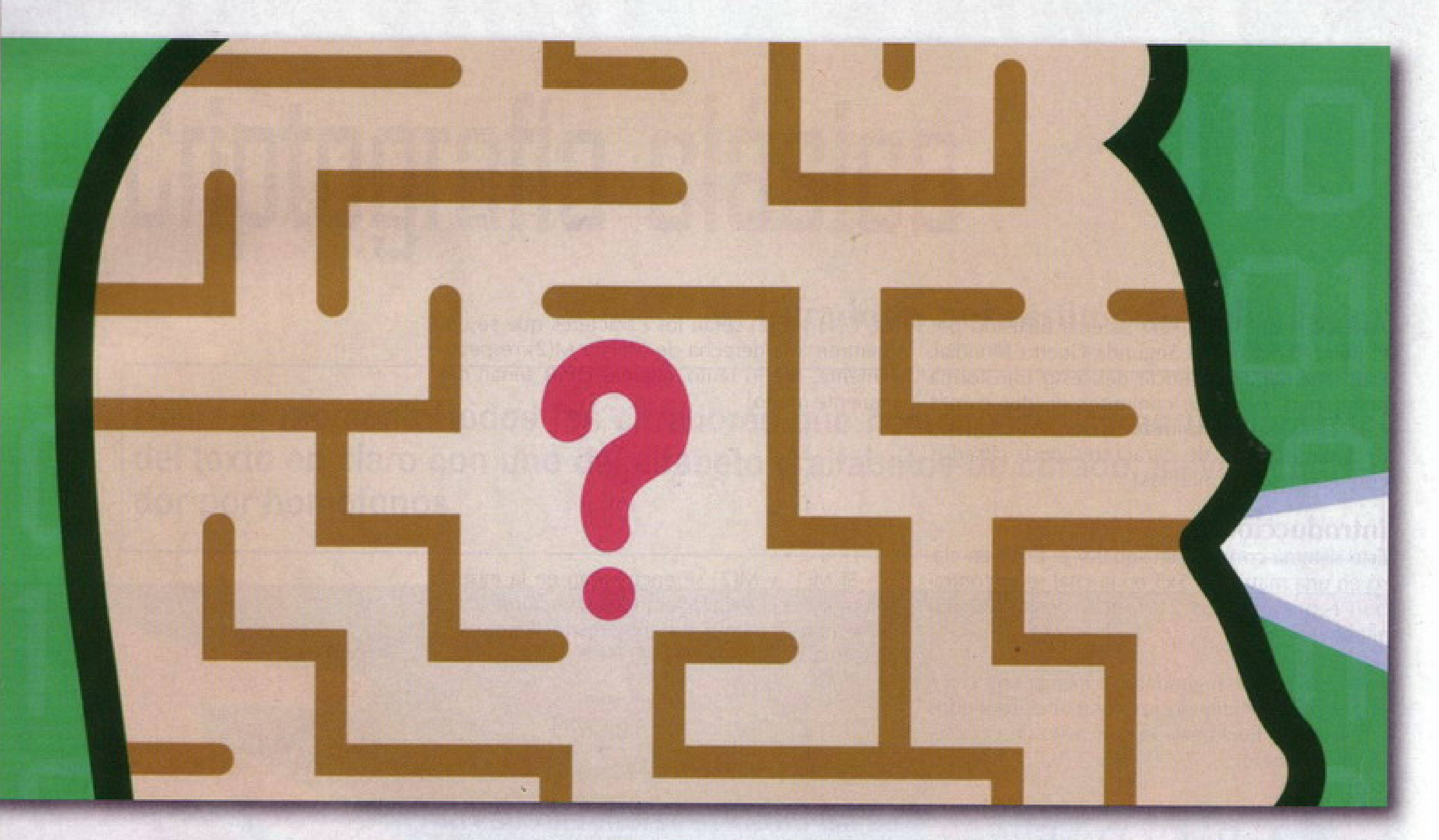
ES IMPORTANTE TENER EN CUENTA QUE NO TODAS LAS MATRICES DE CIFRADO SON DISTINTAS, Y SI LO FUESEN PODRÍAN DAR RESULTADOS IGUALES

3 - Si M(1) y M(2) se encuentran en filas y columnas distintas ambos caracteres formarían dos de los vértices de un rectángulo y entonces C(1) y C(2) corresponderían a los dos vértices que faltan de dicho rectángulo considerando la fila de M(1) como el elemento de C(1). Por ejemplo:

CS - VP
LT - EQ
DZ - HW

4 - En ocasiones podría darse el caso que el poligrama, en este caso de dos unidades, se repitan los dos caracteres y por lo tanto ninguna de las normas anteriores sería válida. Para ello se debe insertar entre ellas algún carácter que identifique fácilmente al lector que ese carácter no es válido, por ejemplo una X, de tal modo que para cifrar "LLAMAS" podría cifrarse "XLLAMAS" de tal modo que se evitaría dicho problema y obtendríamos solución con alguna de las reglas anteriores.

5 - Igual ocurre si el mensaje posee un número de caracteres impar, por ejemplo la palabra "XLLAMAS" que quedaría una S al final, para este caso se recurre igual que en la regla 4, se pondría al final otro carácter, de modo que



quedase "XLLAMASX" y ya no tendríamos ningún problema para cifrarlo.

El descifrado para este sistema es justamente el inverso del cifrado, y por lo tanto las reglas de descifrado serian las siguientes:

1 - Si C(1) y C(2) se encuentran en la misma fila, M(1) y M(2) serán los caracteres justamente a la izquierda, respectivamente.

2 - Si C(1) y C(2) se encuentran en la misma columna, M(1) y M(2) serán los caracteres justamente encima de ellos respectivamente.

3 - Si C(1) y C(2) se encuentran en filas y columnas diferentes, M(1) y M(2) serán los caracteres que se encuentran en los vértices que faltan del rectángulo.

Como ejemplo, para cifrar el texto:

M = CRIPTOGRAFIA CLASICA

Lo convertiríamos en el siguiente para que fuese divisible entre 2:

M = CRIPTOGRAFIA CLASICAX

Y como resultado obtendríamos:

C = APPUZTFSFMMC LAVRPBFA

Criptoanálisis

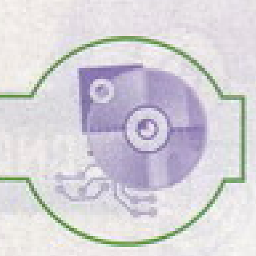
Es importante tener en cuenta que no todas las matrices de cifrado son distintas, y si lo fuesen podrían dar resultados iguales, sobre todo cuando las matrices provienen de otra a la cual se le ha aplicado alguna rotación de filas o columnas.

Además, este sistema presenta un inconveniente y aunque a simple vista parezca que presenta una mayor fortaleza que otros cifrados vistos anteriormente, y para ello se diseñó ese sistema, existe la debilidad de que un mismo conjunto de caracteres, por ejemplo M(1)M(2) se cifran siempre con los mismos caracteres de la matriz de cifrado, por lo tanto presenta semejanzas con cifrados del Cesar. Visto esto es fácil pensar que el sistema puede romperse en base a estadística del lenguaje, utilizando para ellos estadísticas en digramas o Ngramas, de tal modo que podamos reconstruir la matriz de cifrado. Para ello es importante conocer el número de caracteres empleados en la cifra. Si se desconoce este dato se puede probar con trigramas o conjuntos mayores de caracteres.

El ejemplo anterior es demasiado corto para realizar un análisis, pues no se podría obtener ningún análisis de frecuencias y concatenarlos con el idioma español. Con un texto más largo podríamos hacer un análisis e ir averiguando a que filas corresponden ciertos caracteres en función a las reglas antes comentadas.

TheBlooD


fanfilms
Películas por y para los fans



Un fanfilm es una producción audiovisual creada por aficionados sobre un determinado personaje o historia que se distingue de un cortometraje de aficionados por el argumento, normalmente basado en películas, series, cómics o libros fantásticos o de ciencia ficción, cuyos derechos son propiedad de terceros. Es la hora de ver las nuevas correrías de Batman, los Jedis, Indiana Jones, o el capitán Kirk a los mandos del Enterprise.

Las circunstancias especiales del pasado reciente han supuesto un caldo de cultivo perfecto para una nueva generación de individuos que se han beneficiado de un ciclo de prosperidad y crecimiento artístico unido a un período de bonanza económica. El resultado se plasma en todas las áreas de nuestra sociedad, individuos que tienen en común el haber crecido acompañados por las aventuras de Indiana Jones, los héroes de los cómics o las películas de ciencia ficción que marcaron los años 80 y 90 del pasado siglo (eso sin olvidar el resurgir de las películas de superhéroes de los últimos años). Si a esto unimos los últimos avances en tecnología digital, el fenómeno de Internet (y lo que puede suponer como escaparate para nuevas promesas), junto con la falta de creatividad de los grandes estudios de la meca del cine, era cuestión de tiempo que se afianzara lo que ya se conoce como el fenómeno fanfilm.

El fenómeno en sí no nada nuevo puesto que en los años 60 se comenzaron a atisbar los primeros ejemplos. En aquel entonces un estudiante de la universidad de UCLA llamado Don Glut filmó una serie de cortos independientes en blanco y negro basados en aventuras de una serie de cómics de los años 40 y 50. Por la misma época un artista poco conocido llamado Andy Warhol... producía una película llamada "Batman Drácula" (1964) que puede considerarse como un fanfilm, aunque no es hasta los años 70 cuando la popularización en los Estados Unidos de las convenciones de ciencia ficción permitió a los fans enseñar sus propias producciones a la comunidad de fans. El hecho de que no solieran ser obras con permiso de los propietarios de los derechos, hizo que originalmente sólo se proyectasen en convenciones, o se distribuyeran copias piratas que pasaban de mano en mano.

La disponibilidad de cámaras económicas y herramientas de edición de vídeo en ordenadores domésticos permite la realización de películas a cualquier persona que disponga del tiempo necesario y pueda organizar un grupo de personas suficientemente numeroso. Por otro lado, hoy en día se cuenta con la inestimable ayuda de los servicios de streaming de vídeo (como YouTube o Google Video) que consiguen hacer llegar las películas de fans a cada vez más personas. Internet es así un lugar perfecto para los que buscan un rato de fama, homenajear a sus ídolos,



TheForce.net agrupa muchos de los mejores cortos realizados hasta el momento



StarWars Revelations es un fanfilm de altísima calidad

Lo que se grabe en un fanfilm no tiene por qué tener nada que ver con la trama original y por supuesto no se considera "oficial". De la misma forma no tiene ninguna repercusión en el universo ficticio de la serie original ni ha de ajustarse a los cánones determinados por los autores originales o los custodios de la línea argumental. De esta manera es posible encontrarse con auténticos homenajes, serios y fieles a los originales, variaciones igual de serias sobre la trama original (mezclando personajes de varias sagas), y todo tipo de divertidas parodias, pequeñas producciones y escenas realizadas de forma casera sin mayores pretensiones, y otras que alcanzan el rango de miniproducciones profesionales, al involucrar a profesionales del medio que dedican parte de su tiempo libre a participar en este tipo de proyectos.

o llamar la atención de la industria con un producto que puede considerarse como un buen currículum cinematográfico (prueba de ello es el salto a grandes producciones de muchos de los directores envueltos en estor proyectos). Y es que la globalización de la red ha posibilitado que sean conocidos mundialmente, normalmente a través del boca a boca, siendo distribuidos en webs de vídeos, o programas P2P.

Los fanfilms pertenecen al ámbito de la fanfiction, es decir, líneas argumentales realizadas por terceros sin el consentimiento del propietario de los derechos. En el caso de Star Wars, por ejemplo, la productora promueve la realización de fanfilms organizando concursos en su página web (el único requisito es que deben ser comedias o parodias sobre el tema) pero no siempre es así y, en lugar de estar tolerados por el propietario de los derechos o promovidos por este de alguna forma, pueden ser vistos con cierto recelo como ocurre con Paramount o DC Comics que durante cierto tiempo han intentado evitar la proyección de fanfilms basados en Star Trek o Batman, pese a que en la actualidad parece que son más permisivos.



SinCity de Frank Miller ha servido de inspiración para varios autores

Puesto que para realizar un fanfilm es conveniente aunar los esfuerzos de muchas personas (para el vídeo, música, efecto, actores...), lo habitual es que termine haciéndose en base a un tema popular. De ahí que lo que más abunda tenga que ver con series que aglutinan a una gran cantidad de aficionados, como lo pueden ser las sagas de "La Guerra de las Galaxias" o "Star Trek" seguido de cerca de los superhéroes del mundo de los cómics, si bien también podrás encontrar cortos de Galactica, Doctor Who, los Cazafantasmas, Buffy la Cazavampiros o Angel, por ejemplo.

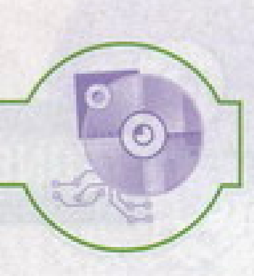
Su duración va desde unos pocos minutos hasta la de una película comercial, aunque muchas veces se opta por hacer un tráiler de una película imaginaria. En cuanto a su calidad puede ser la de un humilde vídeo casero hasta una gran superproducción que pueden llegar a competir con en calidad con el original.

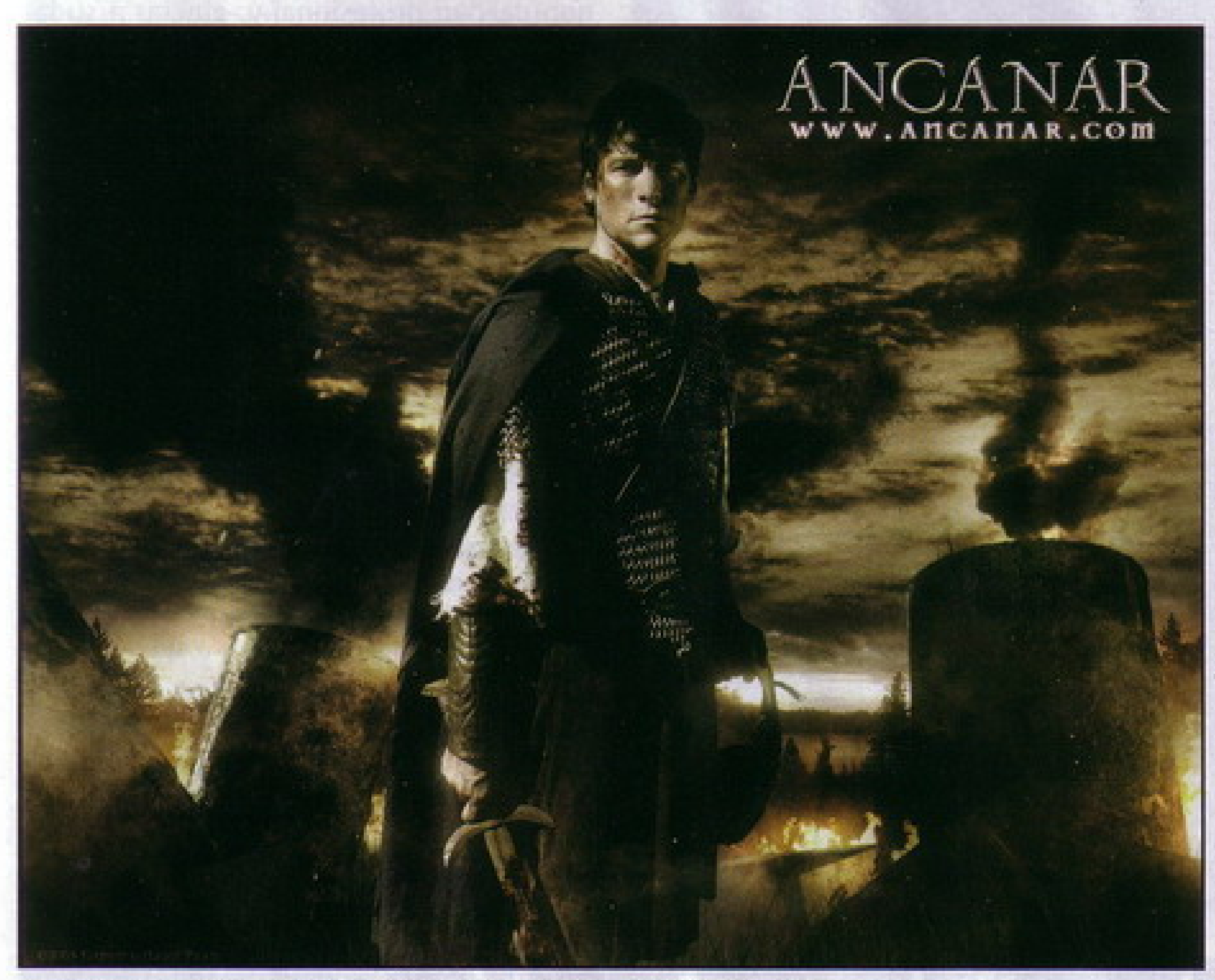
La mejor forma de entender lo que es en sí el fenómeno fanfilm es visionándolos, y puesto que el papel aún no permite la reproducción de material multimedia (tiempo al tiempo), lo mejor será ir repasando por escrito los mejores fanfilms existentes.

Que la fuerza te acompañe

Indudablemente la saga de "La Guerra de las Galaxias" se lleva la palma en lo que a popularidad se refiere. Por ello es lógico que sea la que más de que hablar en este mundillo y de la que se haya logrado resultados más que destacados. Ya en 1997 Kevin Rubio dirigía un clásico de nombre "Troops" (tropas), una excelente parodia del clásico programa de policías Cops (aquella en la que unos periodistas acompañaban a policías en sus pesquisas al son de la pegadiza música de "Bad boys") que nos relata lo que ocurre cuando los Stormtroopers (los soldados del Imperio) salen a patrullar por las peligrosas dunas de Tattooine alternando con rateros jawas y resolviendo peleas que se producen en algunas granjas. En total 10 minutos muy originales.

"Star Wars Broken Allegiance" es una producción del 2003 de casi media hora que nos sitúa entre los episodios IV y V en la que dos aprendices Sith se escapan y son perseguidos por unos cazarecompensas, mientras que "Star Wars Reign of the Fallen" (2006) nos sitúa en la época de las grandes guerras entre los Sith y los Jedis. Ese mismo año llegaba desde Alemania "Tyridium The True Story", una de las producciones más ambiciosas que tomaba como punto de partida la nave Tyridium, la nave que Han Solo utilizó para llevar sus tropas a la luna-santuario de Endor y desactivar el campo de fuerza que protegía a la segunda estrella de la muerte.





Ancanar está en fase de post producción y es una historia más que prometedora

YA EN 1997 KEVIN RUBIO DIRIGÍA UN CLÁSICO DE NOMBRE "TROOPS" (TROPAS), UNA EXCELENTE PARODIA DEL CLÁSICO PROGRAMA DE POLICÍAS COPS

Sin embargo en el año 2005 se presentaba en sociedad la que ha sido probablemente una de las adaptaciones mejor lograda hasta el momento (para muchos superior al episodio I y II). "Star Wars: Revelations", dirigida por Shane Felux, era el resultado de tres intensos años de trabajo que quedaron plasmados en mediometraje de 47 minutos de duración. Situada temporalmente entre las dos trilogías cuenta el exterminio de los Jedi. Con un presupuesto de alrededor de unos 15.000 euros contó con técnicos de efectos especiales de todo el mundo que hacían su trabajo desde casa y lo enviaban para unirlo en el proceso de edición. Los soldados de asalto, Darth Vader o las batallas espaciales parecen salidos directamente de la mano de George Lucas. No pudo entrar en los premios que anualmente entrega Lucas a los fanfilms de Star Wars debido a que incumple una de las normas básicas (es una película no paródica). Goza de una producción muy lograda y mucho trabajo conjunto, aunque según más de uno el casting de los protagonistas podría haber sido algo más "exigente". Un mucho más desenfadado Felux dirigió en 2006 "Pitching Lucas" que ya pudo competir en los Star Wars Film Awards, consiguiendo por primera vez unir los premios de los fans con el que otorga Lucas en persona.

StarTrek New Voyages incluso cuenta con colaboraciones de actores de la serie clásica

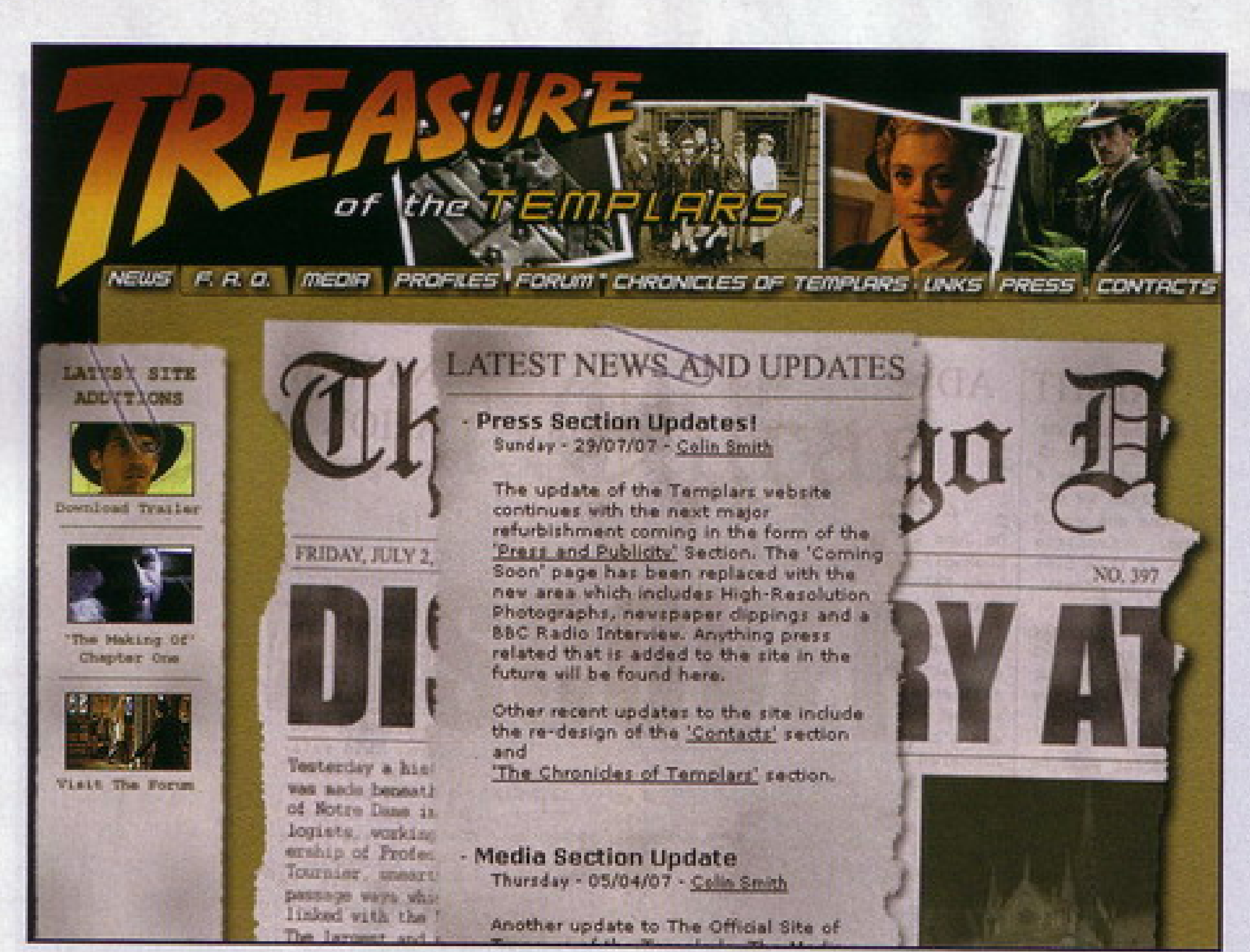
Y siguiendo con las parodias, ¿qué ocurriría si Darth Vader fuera el encargado de un supermercado? "Chad Vader" (2006) de Matt Sloan y Aaron Yonda consta de una serie de episodios donde podrás comprobar cómo serían sus relaciones con su jefe, sus compañeros, sus citas con la cajera... Mucho humor, y homenajes a los mejores momentos del malo malísimo de la saga original.

En el apartado nacional podemos encontrar las "Crónicas de la Vieja República" (2004) de Adolfo Schreier que con apenas 150 euros ha realizado este primer episodio de lo que se pretende sea una serie de varios capítulos. También destaca "Star Wars: THX", otro tráiler teaser español de un proyecto en producción que apunta maneras (por lo visto la fase de rodaje ya ha terminado y se encuentra en fase de post producción). Más recientemente, en 2007, desde Chile nos llegaba de la mano de Inti Carrizo-Ortiz "Star Wars: Renacimiento", el tráiler de un cortometraje, aún en preparación, que puede dar mucho de qué hablar. Nacido en un foro sobre la saga, este proyecto nos contará como algunos Jedi se resisten al exterminio tras la caída de la República.

Star Trek

Pero no todo lo que se desarrolla en el espacio tiene que ver exclusivamente con la Guerra de las Galaxias. Son millones los fans a lo largo y ancho del mundo que siguen las correrías de la nave estelar Enterprise, Voyager o las distintas Deep Space creadas por Gene Rodemberry y popularizadas en las series y películas de Star Trek. El primer gran proyecto asociado a esta saga fue "Starship Exeter" (2002) del que ya se han realizado tres capítulos. La serie sigue los pasos de los viajes de la nave Exeter, conducida por el capitán Garrovick, un personaje que apareció en la serie clásica de Star Trek, y se ajusta en todo lo posible a la serie original.

En el 2004 aparecía "Star Trek: New Voyages" de Jack Marshall, una magnífica serie que ya consta de cinco capítulos y cuyo alto nivel ha permitido que participen en ella Walter Koenig y George Takei, volviendo a encarnar a los exóticos Chekov y Sulu, y Denise Crosby (Tasha Yar de la Nueva Generación que aparecerá en el capítulo que se está finalizando). La serie pretende continuar la saga original, en lo que habría sido la quinta temporada. El aspecto visual y los actores están muy cuidados, convirtiéndola en una serie indispensable para todo trekkie que se precie. Los efectos especiales tie-



IndianaJones va en busca del tesoro de los templarios en este fanfilm

nen calidad profesional y, gracias a su labor, Jack Marshall ha conseguido ser coordinador de efectos especiales en la nueva serie Galáctica. Incluso en la cuarta temporada de la serie Enterprise se utilizó un set en el que se rueda New Voyages para recrear el puente de una nave del siglo XXIII lo que da una idea del nivel del fanfilm. En la red ya es posible encontrar algunos capítulos traducidos y subtitulados al castellano.

Por último, en este apartado tenemos "Star Wreck: In the Pirkinning", una parodia finlandesa del 2005 que mezcla Star Trek y Babylon 5 y que muestra las batallas espaciales más espectaculares que se han visto hasta el momento en un fanfilm. La película de 1 hora y 43 minutos de duración puede descargarse libremente con subtítulos en más de 15 idiomas y ha sido distribuida en varios países en formato DVD convirtiéndola posiblemente en una de las películas finlandesas más exitosas.

>>> Preparados, listos, ¡Acción!

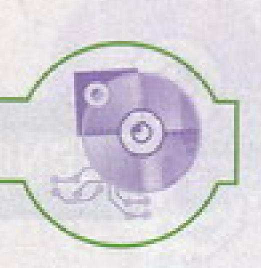
Los avances que se han realizado en tecnología digital son los que han permitido que casi cualquiera pueda llevar a cabo el montaje de una producción cinematográfica. Para empezar podemos beneficiarnos de lo asequible que están las cámaras digitales en la actualidad.

Por otro lado ya no es necesario utilizar costosas mesas de mezclas ni complicados sistemas con los que organizar grabaciones simultáneas de vídeo. Por si fuera poco las herramientas de edición de vídeo permiten montar secuencias de una forma sencilla, al alcance de casi cualquiera. Los programas más utilizados por los aficionados suelen ser el Pinacle Studio o también Adobe Premiere, soluciones bastante fáciles de dominar, aunque siempre se puede elegir dar el salto a otro tipo de herramientas más profesionales que lograrán resultados más espectaculares aunque también exigirán de una mayor curva aprendizaje, aunque para la mayoría de los casos montajes con las herramientas de Pinacle o Adobe serán más que suficientes.

Si hay algo que caracteriza una producción fanfilm es su afán por emular una temática asociada al mundo de la ciencia ficción o el mundo de la fantasía (sería cuanto menos curiosos ver un fanfilm de Falcon Crest, por ejemplo) de manera que los efectos especiales también deben ser considerados como un elemento más del vídeo. Aquí entran en juego varios factores ya que el ingenio está a la orden del día y en ocasiones sustituye de forma más que satisfactoria las carencias de una producción de este calibre. Trucos con espejos, ángulos estudiados, maquillaje, efectos de sonido y una correcta mezcla de las secuencias puede conseguir resultados realmente espectaculares (y si no que se lo digan a Sam Raimi cuando se dio a conocer con la saga de Posesión Infernal que, sin ser un fanfilm sino una producción de terror de bajo coste, supuso toda una revolución para una película cuasi-amateur, de escasos recursos económicos aunque, eso sí, mucha imaginación). En este apartado es donde se requiere de una mayor iniciativa para lograr sacar el máximo provecho a los normalmente escasos recursos de los que dispongamos.

Existen fanfilms que mezclan con éxito efectos en 2D con otros en 3D, acompañados de complejos efectos de sonido, aunque seguramente el mundo del 3D es el que más ha avanzado y el que más provecho ha encontrando en este área. Para crear efectos 3D existen muchas herramientas profesionales que pueden utilizarse (como 3DStudioMax o Maya) aunque suelen tener un coste elevado por lo que la mayoría suele recurrir a aplicaciones más económicas. Por ejemplo podrás encontrar soluciones muy amigables y económicas con las que obtener resultados casi tan buenos. Animation Master es uno de ellos aunque en los últimos tiempos destaca una por encima de todas que además es totalmente gratuita (licencia GPL) llamada Blender (www.blender.org) y que ya ha sido utilizado incluso para realizar alguna que otra producción totalmente en 3D de una calidad impecable.

En las películas más elaboradas el vestuario y los decorados bien logrados añaden un toque adicional de autenticidad. En el caso de los grandes clásicos que se quieran emular, si logran reproducirse con fidelidad hacen mucho más por el resultado final que un efecto añadido digitalmente. En cuanto a los decorados normalmente son simulados en madera, un material empleado para elaborar los escenarios, las armas, paneles de ordenadores o cualquier cosa que se te pase por la cabeza. Los más profesionales pueden optar por otros materiales que, aunque más caros, pueden conseguir objetos más creíbles.





Este corto sobre Catwoman destacó sobre todo por la modelo que lo interpretó

Por último destacar "Star Trek Hidden Frontier" desde cuya página podrás descargarte 7 temporadas con más de 49 episodios filmados, superando en cantidad a muchas series comerciales.

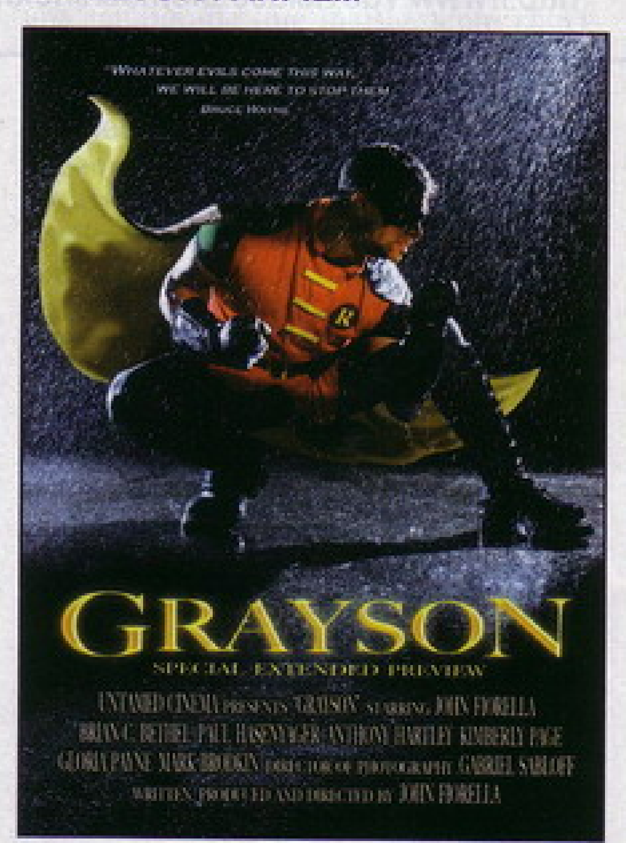
La fuente inagotable de los cómics

Estos últimos años han visto el resurgir del mundo de los superhéroes, un género cinematográfico maltratado en los años 70 y 80 (¿quién no recuerda al casposo Spiderman de los 70?) debido fundamentalmente a las carencias tecnológicas del momento. Hoy, taquillazos mundiales como los X-Men o los 4 fantásticos, han reverdecido un género hasta entonces muy maltratado.

En este apartado Batman es probablemente uno de los héroes más versionados. Como prueba de ello podemos encontrar al director Aaron Schoenke que, aunque cuente con varios cortos muy interesantes ("Patient J" sobre el Joker, o "Batman: Dark Justice"), destaca sobremanera el falso trailer "Batman Legends" (2006) en el que se narra la muerte de Robin y cómo Batman buscará venganza contra su galería de villanos (ha extraído algunos planos del propio cómic en el que se basa esta historia). Como curiosidad el doble de the Rock participa interpretando a Bane, la descerebrada masa de músculo.

El nombre de Sandy Collora en el mundo de los fanfilms es ya toda una celebridad gracias en gran parte al corto "Batman: Dead End" (2003) que fue considerado durante mucho tiempo como el mejor fanfilm. Este director, que ha sido parte del equipo de efectos especiales de películas como Dogma, el Cuervo o Men in Black, realizó este impactante corto en busca de una oportunidad para dirigir. El look de Batman, estéticamente el más fiel al cómic, el del Joker (un actor secundario habitual en la serie "Los Problemas Crecen") es más que convincente, y los Aliens y Depredadores (si, si, no va de coña) que también aparecen son también muy realistas. Poco después, en 2004, Sandy Collora presentaba "World's Finest", un falso tráiler en el que Batman y Superman deben unir fuerzas para enfrentarse a Dos Caras y Lex Luthor. Calidad a raudales y todo un homenaje para los aficionados a los cómics insinuando una historia que seguro sería todo un éxito en la gran pantalla.

SANDY COLLORA ES YA TODA UNA CELEBRIDAD GRACIAS EN GRAN PARTE AL CORTO "BATMAN: DEAD END", CONSIDERADO DURANTE MUCHO TIEMPO COMO EL MEJOR FANFILM



En Grayson puedes ver un tráiler imaginario basado en la historia de Robin

John Fiorella es otro de los "grandes" en el universo de los fanfilms gracias al espectacular tráiler "Grayson", filmado en el 2004, en el que puede verse la historia del Robin original (Dick Grayson) que, tras la muerte de Batman se centra en la búsqueda del asesino. En su camino se cruzan varios villanos como el Joker, Riddler, el Pingüino, Catwoman... y un malvado Superman. Del lado de los buenos están el fiel comisario Gordon y Batgirl, aunque destacan las apariciones especiales de Wonder Woman o Linterna Verde. Un extenso elenco de personajes en una realización impecable que ha permitido a su autor ser después director de segunda unidad del thriller Cherry Crush. Asimismo Allan Agustin terminaba en 2006 "Batman: Knightfall", un corto en formato de dibujo animado basado en la miniserie del cómic en la que Bane le rompe la espalda a Batman, y éste debe buscar un sustituto. Pese a que la animación (basada en el de la serie de animación) es muy mejorable, hay que destacar que en este proyecto sólo ha estado involucrada una persona por lo que el resultado tiene mucho mérito.

La Mujer Maravilla, de la que ya se prepara una adaptación de gran presupuesto en Hollywood, es la protagonista de "Wonder Woman: Balance of Power", un fanfilm de casi 40 minutos de Ron Santiano que goza de una esmerada producción. Muestra las aventuras de la heroína en busca de un poderoso dispositivo con todos los aditivos propios de este personaje (su compañero Steve Trevor, la isla de las Amazonas y hasta un breve cameo al final de Clark Kent). También forma parte, aunque de forma mucho más "naif", del elenco de "Fast Times at Hero High" (Kyle Peck, 2003), una humilde y simpática parodia sin pretensiones (un

>>> Enlaces

Troops	http://theforce.net/troops/
Star Wars Broken Allegiance	http://www.brokenallegiance.net/
Star Wars Reign of the Fallen	www.reignofthefallen.com
Tyridium The True Story	http://www.tydirium.tv/
Star Wars: Revelations	www.panicstruckpro.com/revelations
Pitching Lucas	http://www.atomfilms.com/film/pitching_lucas.jsp
Chad Vader	http://www.blamesociety.net/chadvader/
Crónicas de la Vieja República	www.laviejarepublica.com/
Star Wars: THX	http://www.campanilla.info/?p=417
Star Wars: Renacimiento	http://www.renacimientofilm.com
Starship Exeter	http://www.starshipexeter.com/
Star Trek: New Voyages	http://www.startreknewvoyages.com/
Star Wreck: In the Pirkinning	http://www.starwreck.com/
Star Trek Hidden Frontier	http://www.hiddenfrontier.com/
Batman Legends	http://www.batinthesun.com/
Batman: Dead End	http://www.collorastudios.com
World's Finest	http://www.collorastudios.com/projects/finest/finestmain.htm
Grayson	http://www.untamedcinema.com/
Batman: Knightfall	http://www.youtube.com/profile?user=afterlife2k
Wonder Woman: Balance of Power	http://www.redcapecinema.com/
Fast Times at Hero High	http://www.ifilm.com/video/2483385
Catwoman: Copycat	http://www.youtube.com/watch?v=eTsGZ4uFSuA
Lobo Paramilitary Christmas Special	http://www.youtube.com/watch?v=t9ooZYjF0ml
Watchmen: Page 5	http://www.youtube.com/watch?v=w14DoxRIXW4
Rats	http://www.pitchfilms.com/
Tomorrow's Memoir	http://www.tomorrowsmemoir.com/
Fight of the Universe	http://www.youtube.com/watch?v=4t8H6NS50F8
Born to Hope	http://www.bornofhope.com/
Ancanar	http://www.ancanar.com/
Treasure of the Templars	http://www.treasureofthetemplars.com/
Galactica:	http://www.battlestarfanfilms.com
Waiting for Serenity	http://sigil777.com/Waiting_for_Serenity
V de Vicioso	http://www.vdevicioso.biomachinoid.com/

poco cutre, todo hay que decirlo, pero original) en la que los superhéroes van al instituto. Con homenaje a la famosa escena de Phoebe Cates en Aquel Excitante Curso, vemos los inicios del torpe Hulk, la popular Wonder Woman, el inadaptado Flash, el colgado de Thor o el marchoso John "Green Lantern" Stewart. Cabe destacar que el director de este fanfilm ha sido luego asistente de producción en la Telaraña de Carlota y se dice que también de la futura cinta sobre los Pitufos.

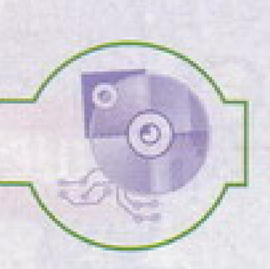
En el año 2006 aparecía una adaptación de Catwoman llamada "Catwoman: Copycat" un fanfilm de apenas 5 minutos cuyo éxito radica, además del homenaje evidente, por lo bien que le queda el traje de latex a Amber Moelter (no así Batman que también aparece según sugieren las fotos promocionales). Dirigido por Collin Blakeston, el corto lleva mucho tiempo en preparación. Mientras, su director trabaja como director de fotografía en la película Bad Blood.

Como puede verse, el mundo de los cómics es una fuente inagotable de personajes e historias que está esperando emerger al celuloide. Más si cabe cuando los responsables difunden que no piensan llevar determinado personaje o historia al cine. Así ocurrió cuando DC Comics anunció que no pensaba llevar a la gran pantalla el cómic en el que Lobo es encargado de asesinar a Santa Claus. Finalmente Scott Leberecht dirigió en 2002 "Lobo Paramilitary Christmas Special", un proyecto en forma de cortometraje realizado como actividad en el American Film Institute, con más de 2000 dólares de presupuesto y protagonizado por Andrew Bryniarski (Zangief en Street Fighter y Cara de Cuero en las nuevas versiones de la Matanza de Texas). Leberech es un especialista en efectos especiales que ha participado en producciones de gran presupuesto como Sleepy Hollow o Spawn.

La prueba de que no siempre es necesario disponer de mucho dinero para realizar algo llamativo lo podemos encontrar en el trabajo del joven autor Bryant Hodson (2005) que con muy pocos medios ha adaptado la quinta página del mítico cómic de Alan Moore y Dave Gibbons llamado muy acertadamente "Watchmen: Page 5" (protagonizado por Rorschach) al estilo Sin City. Se trata de un fanfilm de apenas un minuto filmado como proyecto ¡en el instituto! Como curiosidad hay que destacar que esta joven promesa no es partidaria de que los cómics se adapten a la pantalla (incluso se sintió mal haciendo éste) aunque, visto el resultado, de no seguir con proyectos similares nos podríamos perder un valor emergente.

El mundo de Frank Miller, del que hemos podido ver recientemente adaptaciones muy visuales, sirvió también de inspiración a David Brocca para que en 2004 elaborara el corto "Rats", basado en uno de los relatos dentro del universo de Sin City (pero realizado antes de que se estrenase la película).

Asimismo hay que destacar a Jim Cliffe, guionista y dibujante de cómics que se ha lanzado a la dirección con bastante acierto a través del cortometraje "Tomorrow's Memoir" (2004). De estética



"noir", muestra el ocaso de uno de los héroes más grandes de todos los tiempos. ¿Por qué lo dejó? ¿Quién le sigue? ¿Quién es el narrador? Resuelve los enigmas poco a poco a medida que transcurre la original historia.

De todo un poco

El cine en general sirve de inspiración para este fenómeno aunque parece claro que hay una clara tendencia por escoger temáticas fantásticas o de ciencia ficción. De ahí que películas como Terminator o Matrix también hayan "sufrido" en sus propias carnes esta nueva tendencia cinematográfica. Así aparecía en el 2006 "Fight of the Universe", un pseudo-fanfilm que realmente consiste en la unión de escenas de Robocop, Batman, the Matrix o el Ataque de los Clones para crear al final una lucha entre héroes. Se trata de una variante de fanfilm en la que destaca sobre todo la parte de la lucha entre Robocop y Neo (existe otra entre Terminator y Robocop excelente) que puede encontrarse en la red como un corto independiente, mientras que el resto es un re-montaje de las luchas entre Neo y el Agente Smith.



En Grayson puedes ver un tráiler imaginario basado en la historia de Robin

El universo de Tolkien tiene también su pequeño apartado en el mundo de los fanfilms y el pasado año hemos podido comprobarlo gracias a "Born to Hope" de Kate Robinson, directora inglesa que ya ha trabajado en películas como los Inmortales III, Tomb Raider o Frankenstein. Lo que iba a ser un corto a presentar en una convención sobre Tolkien se convirtió en un ambicioso proyecto de una hora de duración cuyo presupuesto superado ya las 2000 libras (aunque es probable que finalmente se recorte).

Mención aparte merece el proyecto "Ancanar", un prometedor largometraje situado en la Tierra Media cuyo tráiler nos muestra cómo será (¿?) de espectacular esta película (efectos especiales y música incluida) aunque la falta de fondos para una producción en condiciones está retrasando y enfriando este proyecto independiente más de lo necesario.

Indiana Jones no podía quedarse fuera de esta lista y así lo demuestra "Treasure of the Templars" de Jonathan Lawrence (2007). El director, con tres trabajos completados a sus espaldas incluyendo la película de ciencia ficción Dream Parlor, rodó en California, París y Escocia una película con el héroe popularizado por Harrison Ford como protagonista. 5000 libras de presupuesto para una obra que aunque tiene muy buen aspecto, también tiene en su contra un defecto ineludible: Indiana Jones siempre será Harrison Ford, y ver a otro actor interpretándolo siempre sorprende.

En lo que respecta a productos derivados de la televisión, Firefly fue una serie que mezclaba una estética western con ciencia ficción y que, aunque apenas duró una temporada (fue injustamente cancelada), acumuló fans por todo el mundo haciendo de ella una serie de culto. Firefly fue la serie de televisión más vendida en DVD gracias a lo cual pudo hacerse la película llamada Serenity. En Internet es posible encontrar varios fanfilms aunque destaca por encima de todos "Waiting for Serenity" (2005) que, pese a ser muy amateur, es divertido y tiene un final ingenioso que merece la pena ver, sobre todo para los fans.

Otra serie que también ha gozado de muchos seguidores y que marcó una época es V, de la que hay un tráiler de facturación nacional llamado "V de Vicioso" que nos meterá de lleno en la resistencia hispana contra los lagartos invasores del espacio 20 años después de su llegada a la Tierra.

Como última curiosidad, podrás localizar fanfilms de James Bond organizados en la página Commanderbond.net y MI6.co.uk.

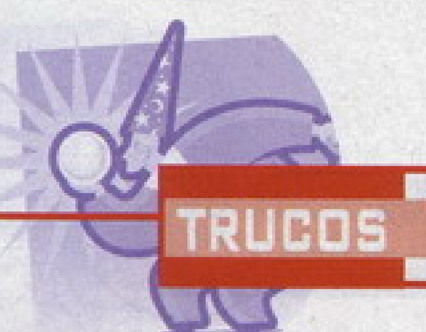
La red como punto de encuentro

Si deseas saber más sobre fanfilms puedes dirigirte a www.theforce.net, una de las páginas más importantes en el mundo de estos proyectos amateurs. En ella encontrarás, además de un amplio listado de películas, una lista de tutoriales para comenzar a rodar un corto. Allí se alojan también muchos fanfilms de La Guerra de las Galaxias. En BatmanFanFilms.com por otro lado podrás encontrar docenas de cortos, tráilers y teasers relacionados con el hombre murciélago. Y si lo que prefieres es buscar directamente películas, la página web www.fanfilms.net dispone de un completo listado de fanfilms organizado por temas. De la misma forma será posible encontrar información en páginas relacionadas con cómics o superhéroes (dada la estrecha relación entre los dos géneros) como pueden serlo webs como Comics2Film.com, o iFilm.

La mayoría de los fanfilms que hemos ido desgranando a lo largo de estas páginas disponen de una página en la que descargar diferentes versiones del mismo con distintas versiones o formatos, aunque también es cierto que si accedes a YouTube, o páginas similares como Google Video, localizarás un número ingente de vídeos que te permitirán estar al día de las últimas novedades en este apasionante fenómeno porque lo que has podido hasta ahora no es más que la punta del iceberg.

Así que ya lo sabes. Si eres de los que desearía contar sus propias historias con tus héroes favoritos, esta es tu oportunidad. Coge tu cámara y, silencio.... se rueda.

Nicolás Velásquez Espinel<

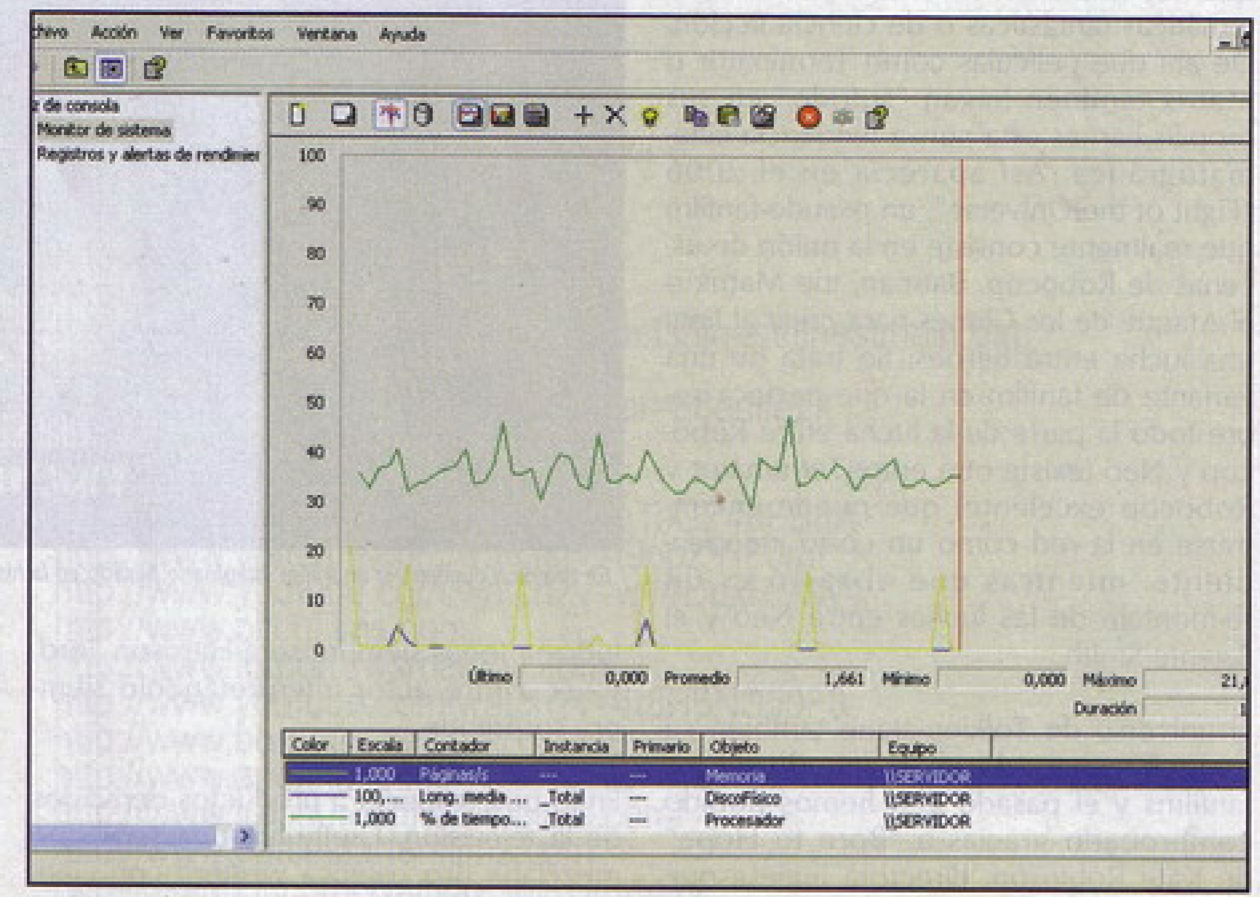


Deshabilitar los Contadores de Rendimiento de Disco

Seguimos en nuestra búsqueda por hallar el método final para optimizar el PC, el Santo Grial de los usuarios que permitirá mejoras sustanciales en el rendimiento del equipo. Esta exploración no es una tarea baladí si no un proceso lento y meticuloso al que podremos colaborar eliminando los Contadores de Rendimiento de Disco.

Durante muchas entregas de esta sección de trucos hemos ido recorriendo toda variedad de métodos para mejorar el rendimiento de nuestra máquina. Conscientes de las limitaciones externas en forma de configuraciones redundantes del sistema o sencillamente servicios innecesarios para nuestro perfil de usuario, que muchas veces coartan nuestras posibilidades, en nuestras manos está el "customizar" determinados parámetros, una acción que en ocasiones logra resultados realmente sorprendentes. Entre los trucos que podemos emplear se encuentran por ejemplo el retocar el archivo de paginación, establecer la prioridad para programas importantes, forzar a dejar de lado los archivos DLL después de cerrar un programa, eliminar programas del arranque de Windows, retocar las directivas locales o deshabilitar servicios innecesarios. ¿Los resultados? Un sistema operativo que ejecuta operaciones más rápido o simplemente que funciona mejor.

Hemos mencionado configuraciones superfluas que desarrollan algunas aplicaciones del sistema y como tal pueden considerarse lo que se conoce como Contadores de Rendimiento. La mayoría conocerá ya el Visor de Sucesos que en alguna ocasión hemos mencionado en esta sección y que nos sirve para localizar determinados fallos o incompatibilidades que puedan registrarse en la máquina. El Visor de sucesos chequea distintas áreas del rendimiento del sistema para analizar posibles errores y localizar incompatibilidades ¿(a alguno le suena el famoso pantallazo azul?) para al final utilizar estos datos en gráficas. En realidad la información allí almacenada proviene de distintos Contadores de Rendimiento, unas herramientas que funcionan en el "backstage" del sistema y que están disponibles tanto para discos lógicos como para discos físicos (esto es útil para determinar por ejemplo qué partición es la causante de la actividad del disco, lo que podría indicarnos la aplicación o servicio que genera determinadas solicitudes, o para el control completo en la monitorización del disco).



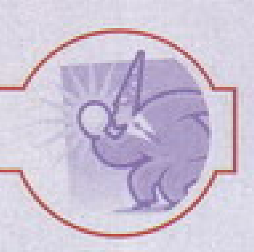
Los Contadores de Rendimiento permiten ver generar los datos de rendimiento

Por supuesto que si no utilizas esta información de forma consciente puede ser una buena idea deshabilitar los Contadores que de otra manera consumirán recursos en el sistema. ¿Y cómo saber si necesitas el contador de rendimiento? Pues bien, aunque parezca una obviedad, si lo necesitas ya lo sabrás, con lo que podemos concluir que en la mayoría de los casos es legítimo dar por hecho que puede deshabilitarse tranquilamente (sólo algunos administradores pueden necesitar realmente la información que proporciona).

Para acceder a la ventana de monitorización que nos muestra la gráfica de datos procedentes de los Contadores de Rendimiento basta con ir a "Inicio - Panel de control". Allí has de localizar el icono correspondiente a "Herramientas administrativas" y, en la ventana que se abra, selecciona "Rendimiento". De la aplicación que se ejecutará, y teniendo marcado en el panel de la izquierda la opción "Monitor de sistema", podrás visualizar en la sección situada a la derecha la información en un formato gráfico y textual.

Como es lógico, el sistema consume una cierta cantidad de recursos en el proceso de monitoreo, un proceso constante que si no se utilizan para nada pueden deshabilitarse para ganar recursos. Para empezar, abre la consola de comandos DOS pulsando en "Inicio - Ejecutar", escribe "cmd" (sin las comillas) y pulsa en Aceptar. En la línea de comandos escribe "diskperf –N". Cuando reinicies el sistema podrás ver cómo los contadores de Rendimiento de Disco estarán deshabilitados. Para volver a dejar el sistema como antes siempre puedes volver a habilitarlos escribiendo en la línea de comandos la siguiente sentencia "diskperf –Y" y luego pulses en Aceptar. Tras reiniciar el sistema todo volverá a quedar como en un principio.

Nicolás Velásquez E.<



Hacer una copia de seguridad de Gmail

Si formas parte de esta realidad (vamos, que vives en nuestro planeta) es probable que seas usuario del servicio de correo gratuito que ofrece Google, Gmail, un sistema de probada eficacia que permite vía web enviar, recibir y gestionar emails y contactos. Pero, ¿qué ocurriría si algún día ya no pudieras acceder a tu correo?



G-Archiver te permite realizar copias de seguridad de Gmail, aunque es de pago

Hay que reconocer que Google ha dado de pleno en su estrategia comercial consiguiendo situar las herramientas que ha ido sacando al mercado en los primeros lugares de popularidad y productividad. Con Google Mail, o Gmail como mejor se le conoce, ha logrado convertirse en una alternativa real a los sistemas de almacenamientos de correo de acceso vía web, como los ofrecidos por Yahoo o Hotmail, por ejemplo, aunque llegando mucho después que estos. Una de las claves de su éxito fue ofrecer inicialmente un espacio de 2GB para almacenar correos, una capacidad "ilimitada" comparada con lo que se podía encontrar por aquel entonces (5, 20 o en el mejor de los casos, qué barbaridad, ¡100 MB!).

Hoy, con 6GB de espacio gratis (y se habla puede ser 9 en breve), el sistema ya en castellano y con decenas de herramientas, ha aumentado sus prestaciones considerablemente (incluso puedes usar cuentas como discos duros virtuales), lo que hace de este uno de los sistemas más utilizados y mejor valorados por la comunidad internauta. Yo, que tuve la suerte de poder probarlo desde que apareciera en su fase beta (en la que sólo podía accederse mediante invitación) me he convertido en un acérrimo defensor de este sistema de correo, aunque eso no evita que exista un riesgo de sufrir algún traspiés que ponga en peligro tus mensajes, como recientemente sucediera cuando Google tomó la decisión de deshabilitar miles de cuentas de usuarios por considerarlas sospechosas de pertenecer a supuestos Spamers, usuarios que se dedicaban a enviar indiscriminadamente mensajes no deseados, también conocidos como mensajes basura. El problema surgió cuando, quienes sufrieron este cierre "forzoso" de sus cuentas resultaron ser usuarios sin culpa alguna que observaron atónicos cómo perdían "en un tris" cientos cuando no miles de valiosos mensajes, adjuntos y contactos. Un contratiempo, por llamarlo de alguna manera, que no deseo ni a mi peor enemigo...

Para sortear este despropósito se hace necesario tomar medidas preventivas con las que proteger nuestra información, y la palabra clave es "copia de seguridad". Aunque existen algunas herramientas en el mercado que nos permiten hacerlo como G-Archiver (http://www.garchiver.com), una interesante utilidad de pago, también existe una alternativa gratuita, disponible desde la propia página del Gmail.

Puesto que la posibilidad de realizar un Backup de emails en Google no viene claramente definida como tal dentro de la propia herramienta, nos veremos obligados a hacer uso de cierto grado de picaresca e ingenio que nos permitan obtener el resultado deseado gracias a que Gmail soporta IMAP. Para ello accede a tu cuenta de correo GMail y desplázate al menú "Configuración -> Reenvío y correo POP". Allí activa la casilla "Habilitar POP para todos (incluso si ya se han descargado)" y guarda los cambios. A continuación ejecuta en tu PC un programa gestor de correo electrónico como Outlook, Windows Mail, Netscape Mail, Eudora o Thunderbird, por citar algunos. En la siguiente página se detalla cómo configurar el acceso para la mayoría de clientes de correo electrónico (¡incluido el iPhone!):

http://mail.google.com/support/bin/answer.py?hl=en&ctx=mail&answer=75726

Una vez configurado le das a "Enviar y Recibir" y se descargará todo el correo con sus adjuntos que tengas almacenado en Gmail (aunque no así los contactos). Además, también podrás enviar y recibir y correos directamente desde el cliente que utilices con los consiguientes beneficios de utilizar este método.

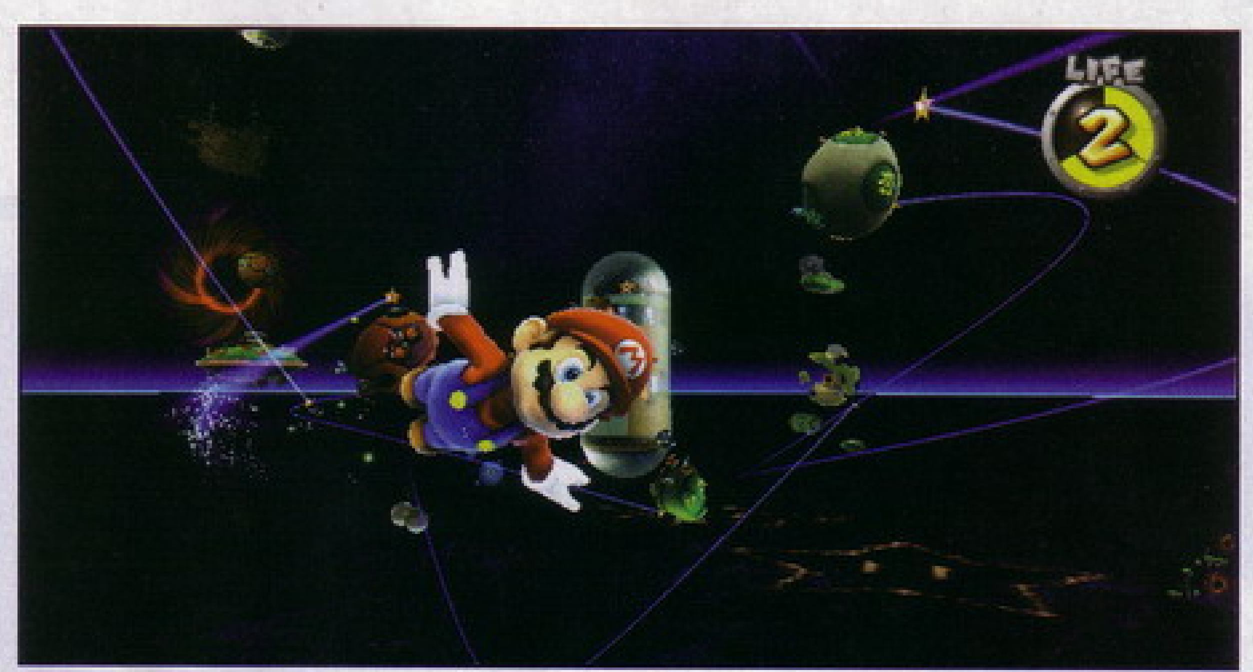
Hay que advertir que en la ayuda disponible online por parte del equipo de Gmail se "sugiere" emplear este método para realizar una copia de seguridad, por lo que los más agoreros ya han empezado a hacer cábalas acerca de un cierre o un cambio en las condiciones de uso del sistema (como podría ser por ejemplo hacerlo de pago). Sin llegar a este extremo nunca está de más salvar nuestros datos cada cierto tiempo para así evitar que la fatalidad pueda jugarnos una mala pasada.

Nicolás Velásquez E.<


SUPER MARIO GALAXY™



Esa sensación de maravilla







Seguramente la expresión ya existía desde hace más tiempo, pero en su día alguien la aplicó para describir con palabras más concretas y comprensibles la llamada "magia de Spielberg". Con esa "sensación de maravilla" se explicaba a las mil maravillas la capacidad del afamado director para evocar y llevar al espectador a mundos y situaciones fantásticas y de ensueño, incluso en las escenas más realistas de su cine. El caso es que, afortunadamente, la sensación de maravilla se ha acuñado y aplicado para otras producciones: libros, discos, otras películas... Y también videojuegos. Gusten o no sus creaciones, Shigeru Miyamoto es otro de esos genios capaces de rodear al jugador en la citada sensación de maravilla durante algunas de sus producciones, que no es poco.

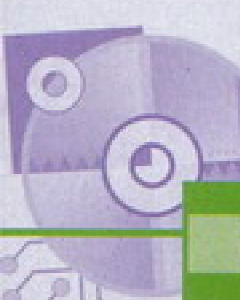
Super Mario Galaxy nace en una situación en la que convergen varios factores. Por un lado, los seguidores de Nintendo esperaban una secuela propiamente dicha del mítico Super Mario 64, un juego capaz de rivalizar con el título que significó la consagración de las plataformas en 3D y que durante años ha estado entre los mejores de la historia. Por otro lado, la enorme masa de usuarios de Wii, que esperaban curiosos qué podía dar de sí una nueva aventura de Mario, independientemente de antecedentes y de filias concretas. Todos los citados, y los que no, pueden darse por satisfechos, porque Super Mario Galaxy es mucho más de lo que unos y otros podían esperar. Es de las pocas veces en las que un esperadísimo juego iguala y supera las expectativas creadas.

Esta nuva entrega huye en muchos sentidos de Super Mario Sunshine, y no solo enlaza con el prestigioso Super Mario 64. A lo largo del juego hay numerosos guiños y cameos de la saga, y además introducidos no solo para satisfacer a los fans, ya que en muchas ocasiones van más allá de la pura anécdota. Técnicamente el juego es lo mejorcito que veremos en mucho tiempo en Wii. No solo gráficamente, el uso del wiimando y del nunchuk, así como los escenarios y los personajes superan con nota lo visto hasta ahora en la consola. En el apartado sonoro, unas melodías orquestadas pondrán la nota épica por momentos, mientras que en otros contribuirán a la sensación de maravilla de marras. Todo un acierto la inclusión de esta nueva banda sonora.

En Super Mario Galaxy de nuevo Bowser ha raptado a Peach, eso que quede claro. Pero esta vez la forma de llegar a nuestra amada es bastante más original que de costumbre. Habrá que recorrerse un montón de planetas, literalmente. Y ahí entra el wiimando, el control de una cámara que puede dar algún quebradero al principio, y las distintas misiones que habrá que ir completando. Estas misiones son más entretenidas que en anteriores entregas, y apuestan más por la acción. También encontraremos minijuegos y otras sorpresas, como la posibilidad de desbloquear a Luigi como personaje jugable en esta aventura. Sea cual sea el motivo por el que nos hemos hecho con una Wii, Super Mario Galaxy es más que imprescindible.

	10
	10
	9
	10
	10
total	10

gráficos · sonido · rapidez · jugabilidad · adicción



Flatpress y Lokicms

Móntate un blog en tu alojamiento gratuito

FlatPress es una buena opción apara montarse un blog, en un espacio gratuito, como los que te regalan con tu conexión a Internet, sin necesidad de disponer de ninguna base de datos ni nada complicado. LokiCMS va más allá es sencillamente el CMS más simple y pequeño que encontrarás.





LokiCMS

Index | Features | Documentation | Themes

Welcome!

LokiCMS is fully Xhtml compliant and adheres to the latest webstandards and is made in php.

LokiCMS is a content management system that is designed to be simple and clear. Most cms systems are way to complicated if you just want to make a small mostly static site, LokiCMS allows you to make a simple site with a few clicks. Right now the entire cms in under 60kb in size. LokiCMS adheres to the lates webstandards and is valid XHTML strict. A validated site ensures that your site will work on every system that supports these standards. One of the best features of LokiCMS is the fact that is does not require a complicated database and instead everything is stored in simple text files, this also makes it easy to install multiple sites on a single host and transferring you site to another locations is just a matter of transferring all the files.

Get LokiCMS

The latest version of LokiCMS is 0.3.0 and you can download it in different formats here:

LokiCMS 0.3.0 (zip 25.3kb)
LokiCMS 0.3.0 (tar.bz2 15.9kb)
LokiCMS 0.3.0 (tar.gz 16.0kb)

Please read the release notes or the readme.txt included in the dowload. Note that this version is unfortunately php5 only.

News

New website address - I am glad to announce that the LokiCMS website has been moved to a new domain, lokicms.com. It is much easier to remember as the old location and offers more room then I think I will ever need. I had to make a new forum as I destroyed the structure of the old one by modifying it some time ago and it was not compatible with the upgrade. I hope this will be the next step for LokiCMS!

New version released - You can now download the next version of LokiCMS. It did not really become what I hoped it would be but is still an improvement over the old version. Changes include full theme support, improved lokicode and security improvements. Also large parts of LokiCMS have been rewritten to be more efficient(faster). I hope you will like the results!

Main site updated - It has been pretty quiet about the next version of LokiCMS but I am happy to announce that I have upgraded this site to LokiCMS 0.3.0 code base. As of now you will not notice much of this but this means that the next version is almost ready. I will add some more information about the changes in it soon.

LokiCMS on the internet - Recently LokiCMS was added to the opensourcecms.com site which is a great site if you want to have take a look to different cms systems that are out there. You can become the admin of every system they list there, a great resource. On google I noticed that LokiCMS has also been added to softpedia, they even made an article on LokiCMS which is very cool! You can check it out here: Softpedia

Forum

You can discuss about LokiCMS on the official forum: LokiCMS forum

La mayoría de los blogeros, empiezan sus pasos en una comunidad gratuita. Al principio esta cubre todas sus necesidades, pero aquellos que se lo toman en serio, al tiempo prefieren disponer de su propio sitio, en el que hacer y deshacer, controlar plugins, themes y cuanto se desee. Para tomar esta decisión no es necesario invertir una gran suma de dinero, al menos, no al principio. De hecho un buen comienzo sería comenzar en un hosting gratuito de los que te regalan con tu conexión a Internet, o con aquel curso que has hecho,... generalmente no incluyen publicidad, y suelen funcionar razonablemente bien para lo que cuestan.

FlatPress

FlatPress es un CMS para blog que no necesita ningún tipo de base de datos, sino que guardar la información de los post y de los comentarios en archivos de texto en uno de sus directorios. El único requerimiento para que funcione, es que el servidor tenga instalado PHP4. Incluye la posibilidad de cambiar y personalizar las plantillas, de hecho posee una buena sintonia con Smarty (smarty.php.net) el motor de plantillas máss popular en PHP. Además dispone una lista de plugins, wiki y blog de la comunidad de desarrolladores y usuarios. Utiliza la licencia GNU GPLv2.

FlatPress Installer

Welcome to FlatPress !

We're very glad you decided to test out our blog. This wizard will guide you through the process of setting up you're brand new unpacked blog, to start blogging right NOW!

Important! Please read ANY part of this wizard as it will give you important informations about the configuration. Also, for the blog and the setup to work properly you'll need your browser to accept cookies, and your server to work properly with sessions.

As a side note, remember this is alpha-quality software, so you may found bugs and holes.

You've been told!

Click *Finish* to start.

Next > | Finish

FlatPress Installer

Create an administrator

Username

Password

Re-type Password

User email

Home Page. URL to your home page or to your blog

Create

Para usarlo en tu espacio web, lo primero que tienes que hacer es descargarlo de flatpress.org y descomprimirlo en tu maquina. Si el inglés no es lo tuyo descárgate la traducción al castellano de joako920.com.ar/proyectos/static.php?page=flatpress y descomprímela igualmente en la ruta de carpetas /fp-interface/langs/ del directorio que se ha creado al descomprimir el primer paquete correspondiente al script.

Ahora solo tendrás que subir por FTP todo el directorio a tu hosting y dar permisos 777 al directorio fp-content. En este momento debes abrir un navegador y visitar la dirección donde se encuentra tu blog, y seguir las sencillas instrucciones que se te daran para instalar el scipt y crear un usuario. Ya tienes instalado tu blog

LokiCMS

Si lo anterior te pareció complicado, y tu lo que en realidad, quieres tener es una pagina sencillita, y complicarte muy poco, puede que tu opción sea este humilde CMS de 25 kb de peso, que editará y creará paginas en sus escuálidas tripas.

Bájatelo en lokicms.com descomprímelo y súbelo por FTP y visita la página install.php. No necesitarás nada más para disponer de este experimento. Un buen comienzo, de una simpleza rotunda.

Mon Magan
monmagan.com



El primer logotipo de SinDominio nada más se puso en marcha el servidor en 1999.

pacio, el cyberpunk, el software libre o el copyleft. Gran parte de lo que hoy se extiende por la blogosfera como "movimiento copyleft" surge también de SinDominio, de la lista de correo copyleft que motivó las primeras Jornadas Copyleft y muchas otras después de ella. También de participantes en SinDominio y de los hacklabs surge la iniciativa CompartirEsBueno.Net.

El futuro ya está aquí

Mucho se habla últimamente de redes sociales para referirse al fenómeno de las webs que permiten algún tipo de servicio al cliente (usuario) para relacionarse con otros usuarios (potenciales clientes) dando a conocer sus textos, audios, vídeos o imágenes. Es lo que se llama la Web 2.0. y promete una interconexión de servicios y personas que está revolucionando la red. Google, Microsoft, Yahoo, etc. se afanan en conseguir crear sus propias comunidades de usuarios. Mientras tanto en SinDominio, así como en muchos servidores o proyectos de software libre, la filosofía de la web 2.0 no es una novedosa "forma de ver la red" sino el mismo punto de partida, el origen de su forma de comprender la red. Por eso desde el principio, y a medida que lo permitía la técnica, SinDominio ha apostado por generar una red de servicios integrados. Sus integrantes disponen de un servidor de Jabber, una correo electrónico, correo vía web, cuenta FTP y un espacio web personal desde hace ya mucho tiempo. Recientemente se ha instalado Drupal como meta-gestor de contenidos de tal manera que cualquier colectivo o persona integrante de SinDominio pueda crear fácilmente una web completa. Y, por supuesto, también se instaló un sistema blogs con Lifetype, que permite una fácil interconexión y que SinDominio tenga su propia comunidad de bloggers, una comunidad que no sólo está comunicada por comentarios, enlaces, sindicación y trackballs sino, sobre todo, por la filosofía de compartir y crear un espacio digital comunitario. Para conocerlo, hay que sumergirse, experimentar y compartir, nada mejor que visitar SinDominio.Net con ganas de navegar un archipiélago de proyectos en red.

EVhAck (evhack.info@gmail.com)

Enlaces

[1] http://www.nodo50.org/contrainfos
[2] http://www.hackmeeting.org
[3] http://biblioweb.sindominio.net/telematica/nonodo50.html
[4] http://acp.sindominio.net o http://madrid.indymedia.org
[5] http://www.hacklabs.org
[6] http://wl0.org/~sjmudd/wireless/madridwireless/article.pdf
[7] http://biblioweb.sindominio.net


Elige tu segundo idioma
Inglés o chino:
2 idiomas clave para moverse por el mundo y competir en el mercado laboral.
Si necesitas hablar inglés, el Profesor Maurer te ofrece la garantía de su famoso Método con el que más de 100.000 personas han aprendido a hablar inglés en sólo unos meses.
Y si lo que necesitas es hablar chino, con el eficaz método para personas que hablan español de la Profesora Yang Yun, lo aprenderás mucho más rápido de lo que piensas.
Elige tu segundo idioma e Infórmate.
CCC The Maurer Method
CCC Yang Yun System Chinese Course
902 20 21 22
www.cursosccc.com
Haz que las cosas pasen.
Para más información, envía este cupón a CCC: Apdo. 17222 - 28080 Madrid
Matricúlate este mes y consigue GRATIS esta estupenda AGENDA ELECTRÓNICA
Sí, deseo recibir información (*)
¿QUÉ CURSO TE INTERESA?
Nombre:
Apellidos:
E-mail:
Teléfono:
Fecha nacimiento:
Domicilio:
Nº:
Piso:
Población:
C.P.:
Provincia:
DNI (opcional):
País de nacimiento:
COMILLAS
CESDE
SANITAS
FeuVert
CEM
8GI
Profesor Maurer
Profesora Yang Yun